ORAL ARGUMENT SCHEDULED FOR JUNE 4, 2014
No. 14-1284

IN THE
UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellant,

v.

ADEL DAOUD,
Defendant-Appellee.

On Appeal From the United States District Court
For the Northern District of Illinois, Case No. 1:12-cr-00723
Honorable Sharon Johnson Coleman

BRIEF FOR APPELLEE

John D. Cline
LAW OFFICE OF JOHN D. CLINE
235 Montgomery St., Suite 1070
San Francisco, CA 94104
Telephone: (415) 322-8319

Thomas Anthony Durkin
Janis D. Roberts
Joshua G. Herman
DURKIN & ROBERTS
2446 North Clark
Chicago, IL 60614
Telephone: (312) 913-9300

Attorneys for Defendant-Appellee
ADEL DAOUD

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Court of Appeals No.: 14-1284

Short caption: United States v. Adel Daoud

Full name of every party represented: Adel Daoud

Names of law firms and lawyers that appeared for the party:

DURKIN & ROBERTS
Thomas Anthony Durkin
Janis D. Roberts
Joshua G. Herman

LAW OFFICE OF JOHN D. CLINE
John D. Cline

Attorney's printed name and address:

LAW OFFICE OF JOHN D. CLINE
John D. Cline
235 Montgomery St., Suite 1070
San Francisco, CA 94104
Telephone: (415) 322-8319
Facsimile: (415) 524-8265
Email: cline@johndclinelaw.com

DURKIN & ROBERTS
Thomas Anthony Durkin
2446 North Clark
Chicago, IL 60614
Telephone: (312) 913-9300
Facsimile: (312) 913-9235
Email: tdurkin@durkinroberts.com

John D. Cline, one of the attorneys
for Defendant-Appellee Adel Daoud

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

CONSTITUTION, STATUTES, AND RULES

OTHER

JURISDICTIONAL STATEMENT

Appellant's jurisdictional statement is not correct in all respects. The district court had jurisdiction under 18 U.S.C. § 3231. This Court has jurisdiction under 28 U.S.C. § 1291 and under the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3 § 7(a). Contrary to appellant's position, mandamus is not appropriate because the government has not shown either that it will suffer "irreparable harm" absent the writ or that it has a "clear right to the writ." *Abelesz v. OTP Bank*, 692 F.3d 638, 652 (7th Cir. 2012).

ISSUE PRESENTED

Did the district court abuse its discretion in ordering disclosure of FISA applications and orders to cleared defense counsel under the protections of CIPA?

This issue has two sub-issues:

1. Did the district court correctly interpret the phrase "necessary to make an accurate determination of the legality of the surveillance" in 50 U.S.C. § 1806(f)?

2. Did the district court abuse its discretion in finding disclosure warranted in this case under § 1806(f)?

STATEMENT OF THE CASE

I. PROCEEDINGS BELOW.

On September 15, 2012, the government filed a criminal complaint charging defendant-appellee Adel Daoud with attempting to use a weapon of mass

destruction in violation of 18 U.S.C. § 2332a(a)(2)(D) (Count One) and attempting to destroy a building by means of an explosive in violation of 18 U.S.C. § 844i (Count Two). A6.[1] An indictment charging the same offenses was returned on September 20, 2012. A4.

A. FISA Notice.

On September 18, 2012, the government filed its "Notice of Intent to Use Foreign Intelligence Surveillance Act Information." R.9. In that filing, the government declared that, under 50 U.S.C. §§ 1806(c) and 1825(d), it "intends to offer into evidence, or otherwise use or disclose in any proceedings in this matter, information obtained and derived from electronic surveillance conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829." *Id*.

B. FAA Issues.

Although the September 18, 2012 notice was limited to FISA, questions arose about the government's potential use of the FISA Amendments Act ("FAA"), which was signed into law on July 10, 2008 and is codified at 50 U.S.C. § 1881a. These questions were spurred by Senate floor comments made by Senator Diane

[1] The record on appeal is cited as "R" followed by the district court docket number. Appellant's Short Appendix is cited as "SA," followed by the page number from the lower right-hand corner of the page. Appellant's Appendix is cited as "A." Appellant's redacted, unclassified opening brief is cited as "G.Br." The defense does not have access to the government's classified brief and thus cannot respond to the arguments it makes in classified form.

Feinstein (Chairman of the U.S. Senate Select Committee on Intelligence) on December 27, 2012, in favor of the reauthorization of the FAA. During her comments, Senator Feinstein suggested that the FAA was used in nine cases, including what she called a "plot to bomb a downtown Chicago bar"—which is a clear reference to defendant's case. Based on Senator Feinstein's comments suggesting that the FAA was used in defendant's case, counsel filed a motion seeking notice of FAA evidence under 50 U.S.C. §§ 1881e(a) and 1806(c). R.42. Through this motion, defendant requested that the government provide notice of: "(1) whether the electronic surveillance described in its FISA Notice was conducted pursuant to the pre-2008 provisions of [FISA] or, instead, the [FAA]; and, (2) whether the affidavit and other evidence offered in support of any FISA order relied on information obtained or derived from an FAA surveillance order." R.42 at 1.

On August 8, 2013, the government filed a "Sur-Reply" to defendant's motion. It acknowledged that notice would be required if the government "intended to use in this case any information obtained or derived from surveillance authorized under [the FAA] as to which the defendant is an aggrieved person." R.49 at 1-2. The government added that no notice was necessary in this case because it "does not intend to use any such evidence obtained or derived from FAA-authorized surveillance in the course of this prosecution." *Id*. at 2.

C. FISA Motion to Suppress and for Disclosure.

On August 9, 2013, the defense filed its motion for disclosure of FISA material and to suppress the fruits of FISA and any other electronic surveillance. R.51 (motion), 52 (memorandum of law). As set forth in the motion, defendant sought to suppress "the fruits of any FISA surveillance and for disclosure of FISA-related materials that may be necessary to litigate motions for discovery and a suppression motion." R.51 at 2. Counsel acknowledged that, without an opportunity to review the FISA applications and any surveillance orders, it was impossible to allege precisely why the government's specific allegations were inadequate. *E.g.*, R.52 at 10, 12. Based on the information available to defendant, counsel did, however, identify eight potential grounds for suppression and disclosure, including the following:

- the FISA applications for electronic surveillance of defendant's e-mail accounts may fail to establish probable cause that defendant, a high school student from suburban Chicago and United States citizen, was "an agent of a foreign power";
- the FISA applications may contain intentional or reckless material falsehoods or omissions, and therefore may violate the Fourth Amendment principles identified in *Franks v. Delaware*, 438 U.S. 154 (1978);
- the primary purpose of the electronic surveillance was to obtain evidence of domestic criminal activity and not foreign intelligence information—or, alternatively, capturing foreign intelligence information was not a "significant" purpose of the FISA surveillance;
- the FISA surveillance may have been based impermissibly on

activity protected by the First Amendment;

R.51 at 3. The motion requested the following relief:

- review all applications for electronic surveillance of the defendant conducted pursuant to FISA;
- order disclosure of the applications for the FISA warrants to defendant's counsel pursuant to an appropriate protective order;
- conduct an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154 (1978); and,
- as a result, suppress all FISA intercepts and seizures, and fruits thereof, derived from illegally authorized or implemented FISA electronic surveillance.

R.51 at 4. Counsel sought disclosure of the FISA materials under the provisions of 50 U.S.C. § 1806(f) and under the due process provision set forth in 50 U.S.C. § 1806(g). R.52 at 24-25. Counsel noted that appropriate security procedures could be crafted to allay any concerns regarding the disclosure of classified material to cleared defense counsel. R.52 at 25. Counsel also argued that *ex parte* proceedings were antithetical to the adversary system of justice, citing *Alderman v. United States*, 394 U.S. 165 (1969). R.52 at 26-29.

On October 25, 2013, the government responded with a 61-page redacted, declassified pleading. R.73. The extensive redactions in the pleading included the majority of the government's substantive arguments and effectively prevented the defense from addressing the government's specific arguments.

In defendant's reply brief, filed on November 25, 2013, counsel cited a number of recently disclosed opinions from the Foreign Intelligence Surveillance Court ("FISC"), which were critical of misrepresentations made by the government in *ex parte* proceedings concerning electronic surveillance programs. R.74.

D. District Court's Order.

As FISA contemplates, the district court, acting *ex parte* and *in camera*, conducted a "thorough and careful review of the FISA application and related materials." SA5. Following that review, the court ordered disclosure to cleared counsel of the FISA application materials. SA5. The court noted that the disclosure would be made "under an appropriate protective order." SA5.

In its order, the court reviewed the relevant FISA procedures. SA1-3. It quoted the standard for disclosure of FISA materials after *in camera*, *ex parte* procedures are triggered by the Attorney General filing his affidavit. SA3-4. The district court recognized that it may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." SA3-4.

Noting that no court had ever allowed disclosure of FISA materials to the defense, the district court found that "in this case" such disclosure "may be necessary." SA5. This conclusion, the court observed, was "not made lightly, and follows a thorough and careful review of the FISA application and related

materials." SA5. Based on its review of those materials, the court found that "an accurate determination of the legality of the surveillance is best made in this case as part of an adversarial proceeding." SA5.

The government's appeal followed.

II. STATEMENT OF FACTS.

At this point in the case, there has been no determination of the facts. The government has detailed its allegations in its complaint. A6. Counsel have proffered the outlines of the defense in an *ex parte* proffer, which has now been unsealed (with the consent of the defense) and made part of the record. R.93. As the defense proffer demonstrates, there is a substantial question, to be litigated at trial, whether defendant was entrapped.

We anticipate the evidence will show that, beginning no later than May 2012, when defendant was eighteen, recently out of high school, and living with his parents, two FBI employees working online in an undercover capacity engaged him in discussion. One FBI employee portrayed himself as a Saudi national who was planning to fight in Syria or Yemen. The other claimed to be an Australian with an interest in "violent jihad." The two undercover FBI employees introduced defendant to an undercover FBI agent posing as an operational terrorist.

Defendant met with the undercover agent six times between July 17, 2012 and September 14, 2012. During the meetings, the undercover agent repeatedly

pressed defendant to come up with ideas for domestic terrorist operations, including identifying specific targets. The agent appealed to defendant's religious beliefs. He went so far as to agree to consult with a fictional sheikh for a "real fatwah" when defendant expressed concerns about a domestic attack, after leaders at his mosque told him that violent jihad was wrong. The recordings of these meetings reveal defendant as naive and gullible.

On September 14, 2012, while in the company of the undercover agent posing as a terrorist, defendant attempted to set off a fake car bomb outside a bar in Chicago. Minutes before the attempt, defendant questioned the agent about whether they could kill women. R.93 at 21. The agent responded, "Yes," and explained that they could do so if the women were paying taxes and supporting the government. R.93 at 21. Defendant asked, "But they never mentioned that women are halal [permissible] to kill. The only, the only brother mentioned that I'm like wait a minute, they also pay taxes and vote. You know. So that's a good . . . oh, so this is just like Palestine?" The undercover agent responded "Yes" and described the United States as a "monster with two heads." R.93 at 22. Minutes later defendant attempted to detonate the fake bomb and was immediately arrested.

SUMMARY OF ARGUMENT

1. The government's argument rests on the premise that the word "necessary" in 50 U.S.C. § 1806(f) plainly means "essential" or "required." That

premise is wrong. As the D.C. Circuit has observed, "The term 'necessary' is a chameleon-like word whose meaning . . . may be influenced by its context . . . .[It] is not language of plain meaning." *Cellco Partnership v. FCC*, 357 F.3d 88, 96-97 (D.C. Cir. 2004)). Courts have given the word a range of meanings, from "helpful" to "essential," depending on its context.

2. The "context" of § 1806(f), including its legislative history and the purposes of FISA, shows that Congress intended the term "necessary" to mean that disclosure would substantially promote the accuracy of the district court's determination of legality—not that disclosure had to be essential or indispensable to an accurate determination. This intermediate interpretation—between "helpful" on one hand and "essential" on the other—is consistent with the authoritative Senate Reports that discuss the term and furthers the statutory goal of balancing civil liberties and national security.

3. By contrast, the Senate Reports specifically rejected the government's interpretation of § 1806(f), under which the determination of legality is *always ex parte* and disclosure is *never* permitted. In addition, that interpretation elevates national security over civil liberties in all cases and thus eviscerates the balance that Congress struck in the statute.

4. Under the correct interpretation of § 1806(f), the district court acted well within its broad discretion in choosing an adversarial process over *ex parte*

proceedings. The government's remaining complaints—that the district court did not precisely track the statutory language in one portion of its order (after reciting that language a page earlier) and did not spell out the "case-specific" (and classified) details of its analysis—amount to the kind of hypertechnical hairsplitting that this Court routinely rejects.

ARGUMENT

In the following Parts, we first address the appropriate standard of review. We then examine the structure and purpose of FISA. Finally, we demonstrate that the district court: (a) correctly interpreted 50 U.S.C. § 1806(f) and (b) appropriately exercised its discretion under that provision—and certainly did not abuse that discretion—in ordering disclosure of the FISA materials to cleared counsel under appropriate CIPA protective procedures.

I. THE STANDARD OF REVIEW.

This Court reviews the district court's disclosure order for abuse of discretion. *See, e.g., United States v. El-Mezain*, 664 F.3d 467, 566 (5th Cir. 2011); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005).

The abuse of discretion standard has two facets in this context. First, the Court reviews *de novo* the district court's interpretation of the phrase "necessary to make an accurate determination of the legality of the surveillance" in 50 U.S.C. §

1806(f). *See, e.g.*, *Tradesman Int'l, Inc. v. Black*, 724 F.3d 1004, 1009 (7th Cir. 2013); *United States v. Young*, 41 F.3d 1184, 1186 (7th Cir. 1994).

Second, the Court will find that the district court abused its discretion in applying the "necessary" phrase to the circumstances of this case "only when no reasonable person could take the view of the trial court." *United States v. Dumeisi*, 424 F.3d 566, 574 (7th Cir. 2005); *see also, e.g.*, *United States v. Harris*, 531 F.3d 507, 514 (7th Cir. 2008) ("We review a district court's denial of a motion for disclosure of the identity of a confidential informant for abuse of discretion and will affirm if any reasonable person could agree with the district court's decision."). As the Court has observed when reviewing other *in camera* determinations, it "rel[ies] particularly heavily on the sound discretion of the trial judge to protect the rights of the accused as well as the government." *United States v. O'Hara*, 301 F.3d 563, 569 (7th Cir. 2002) (quotation omitted) (review of district court's decision after *in camera* review under CIPA); *United States v. Plescia*, 48 F.3d 1452, 1457 (7th Cir. 1995) (affirming district court's refusal to disclose identity of confidential informant after *in camera* review and noting reliance on district court's discretion).

As we demonstrate below, the district court correctly interpreted § 1806(f), and its decision to order disclosure under the circumstances of this case, after "a thorough and careful review of the FISA application and related materials," SA5,

was entirely reasonable. It certainly cannot be said that "no reasonable person could take the view of the trial court." *Dumeisi*, 424 F.3d at 574.

II. THE PURPOSE AND STRUCTURE OF FISA.

Congress enacted FISA in response to *United States v. United States District Court for the Eastern District of Michigan (Keith)*, 407 U.S. 297 (1972).[2] In *Keith* the Supreme Court held that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. The Court noted the intrusiveness of electronic surveillance and cautioned that "[t]he historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Id*. at 317. The Court invited Congress to legislate standards for intelligence-related surveillance that "differ from those already prescribed for specified crimes in Title III." *Id*. at 322.

FISA was also a response to the Report of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee Report),[3] which found that the executive had engaged in warrantless

[2] *See, e.g.*, S. Rep. 604(I), 95th Cong., 1st Sess. 13-14, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3914-16; S. Rep. 701, 95th Cong., 1st Sess. 9, 15-16, *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977, 3984-85.

[3] S. Rep. 755, 94th Cong. 2d Sess. (1976); *see* S. Rep. 604(I), 95th Cong., 1st Sess. 7 (Senate Judiciary Committee Report: "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been

wiretapping of numerous citizens—including journalists, political activists, and members of Congress—who posed no threat to the nation's security and who were not suspected of any criminal offense. The Church Committee Report warned presciently that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature."[4] Thus, FISA "was enacted to create a framework whereby the Executive could conduct electronic surveillance for foreign intelligence purposes without violating the rights of citizens."[5] The Act "was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties."[6]

FISA seeks to accomplish this "sound balance" through several key provisions. First, FISA creates the FISC, to which the government must apply for an order authorizing electronic monitoring, 50 U.S.C. §§ 1803, 1804, or a physical

(continued…)

seriously abused," citing Church Committee report), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908; S. Rep. 701, 95th Cong., 1st Sess. 9 (Senate Intelligence Committee Report with similar remark), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977.

[4] S. Rep. 755, 94th Cong. 2d Sess. (1976).

[5] *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (en banc), *vacated on other grounds*, 543 U.S. 1097 (2005), *reinstated in relevant part*, 405 F.3d 1034 (4th Cir. 2005) (en banc).

[6] *In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (quotation omitted).

search, *id.* § 1823.[7] As the United States Court of Appeals for the Fourth Circuit has observed, "[W]ith certain exceptions . . . a FISA judge must approve in advance all electronic surveillance of a foreign power or its agents."[8]

Second, the statute requires that the Attorney General approve any application to the FISC and that the application contain certain information and certifications.[9] The application to the FISC must include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[10] FISA defines the term "foreign power" to include, among other entities, "a foreign government or any component thereof whether or not recognized by the United States" and "a group engaged in international terrorism or activities in preparation therefor."[11]

An "agent of a foreign power," as applied to a "United States person" such as defendant,[12] means (among other things) "any person who . . . knowingly engages in . . . international terrorism, or activities that are in preparation therefor,

[7] The FISA provisions governing physical searches generally parallel the provisions governing electronic surveillance. Although our argument applies to both sets of provisions, for the sake of simplicity we refer solely to the electronic surveillance provisions.

[8] *Hammoud*, 381 F.3d at 332; *see, e.g., United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988); *United States v. Cavanagh*, 807 F.2d 787, 788 (9th Cir. 1987).

[9] 50 U.S.C. § 1804.

[10] *Id.* § 1804(a)(3)(A); *United States v. Posey*, 864 F.2d 1487, 1490 (9th Cir. 1989).

[11] 50 U.S.C. § 1801(a)(1), (4); *see, e.g., Hammoud*, 381 F.3d at 332 (Hizballah is a "foreign power" under FISA).

[12] *Id.* §§ 1801(i) (defining "United States person").

for or on behalf of a foreign power"; and "any person who . . . knowingly aids or abets any person in the conduct of activities" described above.[13]

The government's application to the FISC must also provide a "statement of the proposed minimization procedures."[14] FISA requires the government to adopt procedures that "are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[15] The minimization procedures must also "require that nonpublicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance."[16] Notwithstanding these requirements, courts have held that the FISA minimization provisions permit the government to record automatically

[13] *Id.* § 1801(b)(2)(C), (E).

[14] *Id.* § 1804(a)(4).

[15] *Id.* § 1801(h)(1). The statute adds that, notwithstanding these provisions, minimization procedures may "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." *Id.* § 1801(h)(3); *In re Sealed Case*, 310 F.3d 717, 731 (Foreign Intelligence Surveillance Court of Review 2002) (discussing FISA minimization procedures).

[16] 50 U.S.C. § 1801(h)(2).

all intercepted communications and to eliminate the non-foreign intelligence information later, when the surveillance tapes are logged and indexed.[17] As a result of this around-the-clock surveillance, FISA wiretaps routinely intercept attorney-client, husband-wife, and other privileged communications.

The government's application to the FISC must contain certain "certifications" by an appropriate executive branch official. Among other things, the official must certify that "a significant purpose of the surveillance is to obtain foreign intelligence information"[18] and that "such information cannot reasonably be obtained by normal investigative techniques."[19]

Third, the statute specifies findings that the FISC must make before it can approve electronic surveillance.[20] The court must find that the procedural requirements of FISA have been satisfied,[21] including the minimization requirements, and it must find (among other things) "probable cause to believe that

---

[17] *See, e.g.*, *Hammoud*, 381 F.3d at 334; *In re Sealed Case*, 310 F.3d at 740-41; *In re Kevork*, 634 F. Supp. 1002, 1016-17 (C.D. Cal. 1985), *aff'd on other grounds*, 788 F.2d 566 (9th Cir. 1986).

[18] The phrase "foreign intelligence information" is defined at 50 U.S.C. § 1801(e). The phrase includes, among other things, (1) "information that . . . is necessary to . . . the ability of the United States to protect against . . . actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power [or] clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power," and (2) "information with respect to a foreign power . . . that . . . is necessary to . . . the national defense or national security of the United States [or] the conduct of the foreign affairs of the United States." *Id.* § 1801(e)(1), (2).

[19] *Id.* § 1804(a)(6)(B), (C).

[20] *Id.* § 1805.

[21] *E.g.*, *id.* §§ 1805(a)(1), (3), (4).

. . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[22] When the target of the surveillance is a "United States person," the FISC must also determine that the government's certifications are not "clearly erroneous."[23]

Fourth, FISA requires notice to the target of the surveillance when the government "intends to enter into evidence or otherwise use or disclose" the fruits of FISA surveillance or a FISA search against an "aggrieved person" in any proceeding in a federal court.[24] FISA defines "aggrieved person" as "a person who is the target of electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[25] Under these definitions, defendant is an "aggrieved person" for the electronic surveillance that targeted him. *See, e.g., United States v. Cavanagh*, 807 F.2d 787, 789 (9th Cir. 1987). The statute authorizes any "aggrieved person" to move to suppress "evidence obtained or derived from" electronic surveillance if "the information was unlawfully acquired" or "the surveillance was not made in conformity with an order of authorization or approval."[26]

---

[22] *Id.* § 1805(a)(2)(A); *see, e.g., Dumeisi*, 424 F.3d at 579; *Hammoud*, 381 F.3d at 332-33 (discussing probable cause requirement).

[23] *Id.* § 1805(a)(4).

[24] *Id.* § 1806(c).

[25] *Id.* § 1801(k).

[26] *Id.* § 1806(e).

When an "aggrieved person" moves to suppress the fruits of FISA surveillance or a FISA search, the Attorney General may file an affidavit that "disclosure or an adversary hearing would harm the national security of the United States."[27] Once the Attorney General files such an affidavit, as Attorney General Holder has done here, 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."[28] Under 50 U.S.C. § 1806(f), any such disclosure must occur "under appropriate security procedures and protective orders."

We discuss the FISA procedures in more detail below.

III. THE WORD "NECESSARY" IN 50 U.S.C. § 1806(f) MEANS THAT DISCLOSURE WOULD SUBSTANTIALLY PROMOTE AN ACCURATE DETERMINATION OF LEGALITY.

The government assumes without analysis that the word "necessary" in 50 U.S.C. § 1806(f) means—indeed, *plainly* means—"essential" or "required." G.Br.19. Its entire argument flows from that premise. But the premise is wrong. As the D.C. Circuit has observed, "The term 'necessary' is a chameleon-like word whose meaning . . . may be influenced by its context . . . .[It] is not language of plain meaning." *Cellco Partnership*, 357 F.3d at 96-97. The "context" of §

[27] *Id.* § 1806(f).

[28] *Id.*; *see also id.* § 1806(g) (if court determines surveillance or search was "lawfully authorized," it shall deny motion to suppress "except to the extent due process requires discovery or disclosure").

1806(f), including its legislative history and the purposes of FISA, demonstrates that Congress intended the term to mean that disclosure would substantially promote the accuracy of the district court's determination of legality—not that disclosure had to be essential or indispensable to an accurate determination.

A. Courts Routinely Interpret "Necessary" To Mean Something Less Than Essential.

Contrary to the government's argument that "necessary" always and plainly means "essential," courts have frequently interpreted the word "to mean less than absolutely essential, and have explicitly found that a measure may be 'necessary' even though acceptable alternatives have not been exhausted." *CT&IA v. FCC*, 330 F.3d 502, 510 (D.C. Cir. 2003) (quotation omitted). Most famously, the Supreme Court confronted the term "necessary" in 1819, when it first interpreted the Necessary and Proper Clause. That provision gives Congress the power

> [t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.

U.S. Const. art. I, § 8. In defining the contours of the Clause, Chief Justice Marshall emphasized that "necessary" does not mean "absolutely necessary." *McCulloch v. Maryland*, 17 U.S. (4 Wheat) 316, 413-16 (1819); *see also, e.g.*, *Jinks v. Richland County*, 538 U.S. 456, 462 (2003) ("[W]e long ago rejected the view that the Necessary and Proper Clause demands that an Act of Congress be

absolutely necessary to the exercise of an enumerated power.") (quotation omitted)). Similarly, in *Commissioner v. Tellier*, 383 U.S. 687 (1966), the Court found that the word "necessary" in the phrase "ordinary and necessary [business] expenses" imposes "only the minimal requirement that the expense be appropriate and helpful for the development of the taxpayer's business." *Id.* at 689 (quotations and brackets omitted).

Cases interpreting "necessary" emphasize that its meaning must be "harmonized with its context." *Armour & Co. v. Wantock*, 323 U.S. 126, 130 (1944). Relying on context, courts have often found "necessary" to mean something closer to "helpful" than to "essential" or "indispensable." *See, e.g.*, *Snider v. United States*, 468 F.3d 500, 513 (8th Cir. 2006) (interpreting "necessary" in 26 U.S.C. § 6103; court rejects "strictly essential" and holds that the "'appropriate or helpful' meaning of 'necessary' is the only practical interpretation in this context"); *Prometheus Radio Project v. FCC*, 373 F.3d 372, 393-94 (3d Cir. 2004) (interpreting "necessary" in § 202(h) of the Telecommunications Act of 1996 to mean "'convenient,' 'useful,' or 'helpful,' not 'essential' or 'indispensable'"); *FTC v. Rockefeller*, 591 F.2d 182, 188 (2d Cir. 1979) (interpreting "necessary" in 15 U.S.C. § 46; court holds that FTC's authority to conduct an ancillary investigation of a bank when "necessary" did not require investigation to be

"absolutely needed" or "inescapable," but instead that it "arise reasonably and logically out of the main investigation").

These cases confirm that the central premise of the government's argument is simply wrong: the word "necessary" does not plainly mean essential or indispensable. Instead, the term must be read together with the phrase in which it is embedded—"necessary to make an accurate determination of the legality of the surveillance"—and in light of both the legislative history of FISA and the statutory purpose. Read in this context, the term means that disclosure would substantially promote the accuracy of the district court's determination of legality—an intermediate interpretation between the extremes of "useful" on one side and "essential" on the other.[29]

B. The Legislative History of FISA.

The legislative history of FISA cuts squarely against the government's insistence that the word "necessary" in § 1806(f) requires a showing that disclosure is essential or indispensable to an accurate determination of legality.

[29] The government relies for its interpretation of "necessary" on a treatise. G.Br.19 (citing 2 David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions* § 31:3, at 263 (2d ed. 2012)) ["Kris & Wilson"]. (The government mis-cites the relevant provision as § 29:3.) But Kris and Wilson rely on the purported "plain meaning" of "necessary," without citing authority for that meaning, and they concede (in an understatement, as we demonstrate below) that what they consider the "plain meaning" of the term "is, however, somewhat at odds with the explanation in the legislative history." *Id.*

Two authoritative Senate Reports—one from the Senate Judiciary Committee and the other from the Senate Intelligence Committee—discuss in detail the provision that became § 1806. The Reports observe:

> The extent to which the government should be required to surrender to the parties in a criminal trial the underlying documentation used to justify electronic surveillance raises delicate problems and competing interests. On the one hand, broad rights of access to the documentation and subsequent intelligence information can threaten the secrecy necessary to effective intelligence practices. However, the defendant's constitutional guarantee of a fair trial could seriously be undercut if he is denied the materials needed to present a proper defense. The Committee believes that a just, effective balance has been struck in this section.

S. Rep. 604(I), 95th Cong., 1st Sess. 53, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3954; *see* S. Rep. 701, 95th Cong., 1st Sess. 59 (similar passage in Senate Intelligence Committee Report), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4028. Turning to § 1806(f), the Committees summed up the disclosure provision as follows:

> The committee views the procedures set forth in this subsection as striking 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.
>
> The decision whether it is necessary to order disclosure to a person is for the Court to make after reviewing the underlying documentation and determining its volume, scope and complexity. The committee has noted the reasoned discussion of these matters in the opinion of the Court in *United States v. Butenko*, [494 F.2d 593 (3d Cir. 1974) (en banc)]. There, the Court, faced with the difficult

problem of determining what standard to follow in balancing national security interests with the right to a fair trial stated:

> "The distinguished district court judge reviewed in camera the records of the wiretaps at issue here before holding the surveillances to be legal . . . Since the question confronting the district court as to the second set of interceptions was the legality of the taps, not the existence of tainted evidence, it was within his discretion to grant or deny Ivanov's request for disclosure and a hearing. The exercise of this discretion is to be guided by an evaluation of the complexity of the factors to be considered by the court and by the likelihood that adversary presentation would substantially promote a more accurate decision." (494 F.2d at 607.)
>
> Thus, in some cases, the Court will likely be able to determine the legality of the surveillance without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which includes [sic] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part since such disclosure "is necessary to make an accurate determination of the legality of the surveillance." [Footnote omitted.]
>
> Cases may arise, of course, where the Court believes that disclosure is necessary to make an accurate determination of legality, but the Government argues that to do so, even given the Court's broad discretionary power to excise certain sensitive portions, would damage national security. In such situations the Government must choose—either disclose the material or forego the use of the surveillance-based evidence. Indeed, if the Government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed . . . .

S. Rep. 604(I), 95th Cong., 1st Sess. 58-59 (footnote omitted; ellipsis in original), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3959-60; *see* S. Rep. 701, 95th Cong., 1st

Sess. 64-65 (identical language in Senate Intelligence Committee Report), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4033-44.

Several points are evident from this passage. First, the Senate Judiciary and Intelligence Committees plainly did not anticipate what followed over the next thirty-six years—that no court would *ever* find the "necessary" standard satisfied. Nothing in the Committees' discussion suggests that they intended that standard to erect an insuperable barrier to disclosure. To the contrary, in choosing a balanced approach, the Committees specifically eschewed "an entirely *in camera* proceeding"—only to have the courts overturn that Congressional intent through an overly strict interpretation of "necessary."

Second, the Committees, through their citation to *Butenko*, placed broad discretion in district judges in determining when disclosure is "necessary to make an accurate determination of the legality of the surveillance." They intended that discretion to be exercised "after reviewing the underlying documentation and determining its volume, scope and complexity"—precisely as the district court did here.

Third, the Committees—again through their reliance on *Butenko*—suggest that the "necessary" standard is met when the district court determines that "adversary presentation would substantially promote a more accurate decision"—a

far lower standard than the "essential" or "indispensable" standard the government advocates.

Fourth, the Committees noted the district court's "broad discretionary power to excise certain sensitive portions" from the FISA materials before disclosure. This recognition of the district court's inherent power to take necessary protective measures now finds a statutory basis in CIPA (discussed below). That power substantially ameliorates the government's professed national security concerns.

Finally, the Senate Judiciary and Intelligence Committees contemplated—and did not shy away from—the outcome the government suggests is intolerable (G.Br.29-30): that the district court would order disclosure, the government would refuse to comply, and the court would suppress the surveillance or dismiss the prosecution. Just as Congress did in CIPA, 18 U.S.C. App. 3 § 6(e), the Committees left the choice with the government: either comply with the disclosure order or refuse and suffer appropriate sanctions.

Two other portions of the legislative history are relevant as well. First, an early version of the definition of "foreign intelligence information" included the words "necessary" and "essential." "Necessary," according to the Senate Judiciary Committee, "requires more than a showing that the information would be useful or convenient." S. Rep. 604(I), 95th Cong., 1st Sess. 31, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3933. "Essential" requires "a showing that the information is

important and required but not that it is of utmost importance or indispensable." *Id*. Thus, "necessary" merely meant something more than "useful or convenient," and not even "essential" required a showing that information was "indispensable."

The Senate Intelligence Committee deleted "essential" from the final definition of "foreign intelligence information" (codified at 50 U.S.C. § 1801(e)). The Intelligence Committee declared that by the term "necessary," it "intends to require more than a showing that the information would be useful or convenient. The committee intends to require that the information is both important and required. The use of this standard is intended to mandate that a *significant need* be demonstrated by those seeking the surveillance." S. Rep. 701, 95th Cong., 1st Sess. 31 (emphasis added), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4000. As Kris & Wilson observe, in practice the word "necessary" in § 1801(e) means little more than "relevant." 1 Kris & Wilson, *supra*, § 8:30 at 299-300.

Second, the minimization procedures in 50 U.S.C. § 1801(h)(2) bar dissemination of nonpublicly available information in a manner that identifies any United States person without the person's consent, "unless such person's identity is necessary to understand foreign intelligence information or assess its importance." The House Conference Report explains that "[b]y 'necessary' the conferees do not mean that the identity must be essential to understand the information or assess its importance. The word necessary requires that a knowledgeable intelligence

analyst make a determination that the identity will contribute in a meaningful way to the ability of the recipient of the information to understand the information or assess its importance." H. Conf. Rep. 1720, 95th Cong., 2d Sess. 23 (Oct. 5, 1978).

The use of "necessary" in §§ 1801(e) and 1801(h)(2) sheds light on the word's meaning in § 1806(f). As the Supreme Court has observed, "[I]dentical words and phrases within the same statute should normally be given the same meaning." *Hall v. United States*, 132 S. Ct. 1882, 1891 (2012) (quotation omitted); *see, e.g., United States v. Robers*, 698 F.3d 937, 942 (7th Cir. 2012). Under this principle, the meanings ascribed to "necessary" in §§ 1801(e), 1801(h)(2), and 1806(f) should be the same. And, according to the legislative history, the meanings are very similar: "significant need" in § 1801(e), "contribute in a meaningful way" in § 1801(h)(2), and "substantially promote" in § 1806(f). These standards are all somewhat higher than "useful or convenient," but far lower than the "essential" or "indispensable" standard that the government advocates.

C. The Legislative Purpose.

A court must construe a statutory term "in a manner consistent with the [statute's] purpose." *Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 118 (2001); *see, e.g., Ryan v. United States*, 725 F.3d 623, 626 (7th Cir. 2013) (where statute is ambiguous, court must "interpret it in the manner most consistent with the

statutory language as a whole, its purpose, and in a manner that will render it constitutional"). As noted above, FISA "was enacted to create a framework whereby the Executive could conduct electronic surveillance for foreign intelligence purposes without violating the rights of citizens." *Hammoud*, 381 F.3d at 332. The Act "was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties."[30] Interpreting "necessary" in § 1806(f) to have the intermediate meaning of "substantially promote" is fully consistent with FISA's effort to balance civil liberties and the need for surveillance—a balance in need of recalibration, as recent events confirm.

1. Protecting Civil Liberties.

The government's interpretation of § 1806(f)—that "necessary" means "essential," and disclosure is *never* "essential"—does nothing to advance civil liberties. To the contrary, a system that operates in secret, with no adversarial input—as the FISA process has functioned for more than thirty-five years—is almost certain to breed abuse.

[30] *In re Kevork*, 788 F.2d at 569 (quotation omitted); *see, e.g.*, S. Rep. 604(I), 95th Cong., 1st Sess. 4 (Senate Judiciary Committee Report notes Attorney General Griffin Bell's view that "this bill strikes the balance, sacrifices neither our security nor our civil liberties, and assures that the abuses of the past will remain in the past . . . ."), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3905-06; *id*. at 7 (bill "goes a long way in striking a fair and just balance between protection of national security and protection of personal liberties"), *reprinted in* 1978 U.S.C.C.A.N. at 3908; *id*. at 9 ("Striking a sound balance between the need for such surveillance and the protection of civil liberties lies at the heart of S. 1566."), *reprinted in* 1978 U.S.C.C.A.N. at 3910; S. Rep. 701, 95th Cong., 1st Sess. 7, 16 (Senate Intelligence Committee Report with similar remarks), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3975, 3985.

The Supreme Court has declared that "'[f]airness 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 opportunity to meet it.'" *United States v. James Daniel Good Real Property*, 510 U.S. 43, 55 (1993) (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). The Court made the same point in *Franks v. Delaware*, 438 U.S. 154 (1978). *Franks* held that a defendant must be permitted to attack the veracity of the affidavit underlying a search warrant, upon a preliminary showing of an intentional or reckless material falsehood. The Court rested its decision in significant part on the *ex parte* nature of the procedure for issuing a search warrant and the value of adversarial proceedings:

> [T]he hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily ex parte, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an ex parte inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

438 U.S. at 169.

The same considerations that the Court found compelling in *Franks* and *James Daniel Good* militate against uniformly *ex parte* procedures in the FISA context. As early as 2002, the FISC acknowledged (in an extremely rare published opinion) that without adversarial proceedings, systematic executive branch misconduct—including submission of dozens of FISA applications with "erroneous statements" and "omissions of material facts"—went undetected by the courts until the DOJ chose to reveal it. *See In re All Matters*, 218 F. Supp. 2d 611, 620-21 (Foreign Intelligence Surveillance Court), *rev'd*, 310 F.3d 717 (Foreign Intelligence Surveillance Court of Review 2002).[31]

Recent revelations provide further evidence that the *ex parte* FISA system has failed to meet the statutory goal of protecting civil liberties. For example, in a FISC opinion dated March 2, 2009, in the matter captioned *In re Production of Tangible Things From [REDACTED]*, Dkt. BR 08-13, Judge Reggie B. Walton of the United States District Court for the District of Columbia documented a number of statutory violations of the NSA's electronic surveillance programs. Judge Walton rejected the government's explanations for the violations and criticized its repeated misrepresentations and non-compliance with FISC orders. *See* R.74 at 5-6.

[31] The FISC was sufficiently alarmed by these erroneous applications that it "decided not to accept inaccurate affidavits from FBI agents whether or not intentionally false," and "[o]ne FBI agent was barred from appearing before the Court as a FISA affiant." *In re All Matters*, 218 F. Supp. 2d at 621.

Similarly, in a declassified FISC opinion dated October 3, 2011, Judge John D. Bates of the United States District Court for the District of Columbia found the NSA's surveillance under the FAA to be "deficient on statutory and constitutional grounds," particularly with respect to the mass collection of emails of American citizens that were entirely domestic and not to or from a foreign intelligence target. Judge Bates also found that the NSA had been acquiring Internet transactions before the FISC approved of such acquisitions. *See* R.74 at 6-7.

Judge Bates found serious problems with the NSA's collection of information in another extensive FISC Opinion, which the DNI released to the public on November 18, 2013. As stated at the outset of this 117-page opinion, Judge Bates reviewed the government's "application to re-initiate in expanded form a pen register/trap and trace (PRITT) authorization for the National Security Agency (NSA) to engage in bulk acquisition of metadata about Internet communications." (p. 1).[32] In reviewing the government's application, Judge Bates cited a number of "serious compliance problems" with the NSA's collection of Internet metadata and its years-long disregard of the limits imposed on it by the FISC. Remarkably, despite the severity of these criticisms of the NSA's failure to comply with the FISC's orders, as well as the NSA's repeated misrepresentations

[32] The government also sought "Court authorization to query and use information previously obtained by NSA, regardless of whether the information was authorized to be acquired under prior bulk PR/TT orders of the [FISC] or exceeded the scope of previously authorized acquisition." (pp. 1-2).

before the FISC, the NSA surveillance programs at issue were ultimately allowed to continue with modifications and reporting requirements. *See* R.74 at 7-9.

Three stark statistics underscore the dysfunction of the current FISA system: (1) year in and year out, the FISC approves without modification the overwhelming majority of the FISA applications the government presents and rejects only a tiny handful—if that—out of more than a thousand;[33] (2) until the district court's order in this case, no court had ever granted defense counsel access to FISA applications and orders under § 1806(f), so no adversarial eye had ever scrutinized them; and (3) no court has ever granted a motion to suppress the fruits of FISA surveillance.

Until recently, some might have argued that these three statistics were unrelated, or that they showed that the government officials who prepared FISA applications had performed near-perfectly for 35 years. But recent developments—including the declassified opinions by Judges Bates and Walton—have destroyed any such illusions. The stark fact is that the FISA system, interpreted by the courts to require ex parte proceedings in *every* case and *never* to grant defense counsel access to FISA applications and orders, has failed to protect

[33] According to the Attorney General's annual reports (available at http://fas.org/irp/agency/doj/fisa), since 1978 the FISC has approved (either as submitted or with modifications) well over 20,000 applications or extensions authorizing FISA surveillance, more than 99% of the total applications submitted. The FISC has rejected outright only a handful of applications, and the DOJ has successfully resubmitted some of those. The statistics for 2013, released a few days ago, are typical: the government made 1,588 applications for electronic surveillance; none were denied or withdrawn; and the FISC modified 34 applications.

civil liberties. Interpreting § 1806(f) as Congress intended, to permit disclosure when adversarial proceedings will substantially promote the accuracy of the district court's determination, marks an important step toward restoring the balance that Congress sought to strike in 1978.[34]

2. Protecting National Security.

The government's principal argument for reading "necessary" to mean "essential" or "indispensable" (apart from its misguided plain meaning argument) is that *any* disclosure of FISA materials, *ever*, to *any* defense counsel, under *any* circumstances, will cause irreparable damage to national security. The Senate Judiciary and Intelligence Committees did not accept that view in 1978, as their Reports confirm. The argument is even more clearly wrong now, following the enactment of the Classified Information Procedures Act ("CIPA") in 1980 (two

[34] Professor Michael J. Glennon of the Fletcher School of Law and Diplomacy at Tufts University has written a recent article titled *National Security and Double Government*, 5 Harv. National Security J. 1 (2014), which, it is suggested, explains why this balance has become so lopsided. Glennon argues, in short, that the President now exercises little substantive control over the overall direction of U.S. national security policy, and that neither Congress nor the courts have the ability to exercise any meaningful oversight, and instead provide only the illusion of accountability. *Id*. at 110. Drawing upon the theory of the 19th Century British scholar Walter Bagehot, Glennon suggests instead this control is exercised by what has effectively become a "double government" network made up of the forty-six federal departments and agencies of millions of employees and a total annual outlay of around $1 trillion, who are engaged in classified national security work whose missions range from intelligence gathering and analysis to what Glennon describes as "war-fighting, cyber-operations and weapons development." Glennon also points out that some 1,271 government organizations and 1,931 private companies work on various programs related to counterterrorism, homeland security, and intelligence in about 10,000 locations in the United States. With operations of such mammoth proportions it is little wonder, Glennon posits, that these bureaucracies have an incentive to "exaggerate risks and pander to public fears—an incentive to pass along vague and unconfirmed threats of future violence, in order to protect themselves from criticism should another attack occur." *Id*. at 27-28 (footnotes and quotations omitted).

years after the enactment of FISA) and the extensive experience that courts, prosecutors, and defense counsel have had with the statute since then.

CIPA contains several provisions that speak to the government's overblown concern that disclosure would endanger national security here. First, it provides for entry of a protective order.[35] The CIPA protective order—the standard terms of which are largely settled after decades of experience—sets the conditions under which defense counsel may review classified discovery, establishes procedures for filing classified pleadings, and prohibits anyone associated with the defense from revealing publicly the classified information to which access is granted. *See, e.g.*, *United States v. Gowadia*, 2010 U.S. Dist. LEXIS 80572 (D. Haw. May 8, 2010) (entering a typical CIPA protective order).

The protective order also appoints Court Security Officers in accordance with the security procedures adopted by the Chief Justice under CIPA § 9(a).[36] Although the CSOs work for the Department of Justice, they are independent of the prosecution team. They advise the parties and the court on the proper handling of classified information, and they serve as conduits for the flow of classified discovery and pleadings among the parties and the court.[37]

---

[35] 18 U.S.C. App. 3 § 3.

[36] 18 U.S.C. App. 3 § 9(a). The procedures, issued by Chief Justice Warren Burger in 1981, appear in a note following CIPA § 9.

[37] *See* 9 United States Attorney's Manual, Criminal Resource Manual § 2054(I)(C) (describing role of CSO).

The CIPA protective order requires defense counsel and other members of the defense team to obtain security clearances before receiving access to classified discovery. The protective order also requires the defense to maintain all classified information in a Sensitive Compartmented Information Facility, or SCIF. The SCIF consists of one or more secure rooms, usually in the federal courthouse where the case is being heard. It is protected by locks and other security devices. The SCIF contains safes to hold classified documents, secure computers on which to prepare classified pleadings, and other approved equipment.

Once the protective order is in place, defense counsel has the necessary clearance, and the SCIF is ready, the parties begin the classified discovery process. CIPA § 4 governs classified discovery. That provision allows the court to authorize the government, "upon a sufficient showing," to delete classified information from the discovery it provides or to furnish substitutions for the classified information in the form of summaries or admissions. The statute adds that "[t]he court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone." 18 U.S.C. App. 3 § 4.[38] The government has already invoked the CIPA § 4 procedures in this case. R.39, 45, 48.

[38] CIPA contains additional procedures governing the use of classified information at trial and in hearings and giving the government a right of interlocutory appeal. *See* 18 U.S.C. App. 3 §§ 5, 6, 7, 8.

CIPA has been in existence 34 years. During that time huge volumes of enormously sensitive classified information have been made available under its strict security measures to cleared defense counsel in scores of federal criminal cases—without, as far as counsel are aware, a serious security violation by the defense. In a case handled by one of undersigned counsel, the CIPA procedures successfully protected nuclear weapon codes that government scientists testified under oath were capable of "changing the strategic global balance" and thus "represent[ed] the gravest possible security risk to the United States." *United States v. Lee*, 2000 U.S. App. LEXIS 3082, at *5-*6 (10th Cir. Feb. 29, 2000). If the CIPA procedures could adequately protect those secrets (and other sensitive classified information in many other cases), they can surely protect the secrets contained in the FISA materials that the district court has ordered disclosed.

Apart from an unfounded and insulting suggestion that cleared defense counsel cannot be trusted with classified information, G.Br.28-29 n.15, the government rests its "national security" argument (or at least the portion that defense counsel are permitted to see) on the contention that, despite having the requisite security clearances, defense counsel lack a "need to know" the classified information contained in the FISA materials. G.Br.27-29. The government's argument is circular. If this Court affirms the district court's disclosure order, then counsel will have a need to know the FISA information to adequately defend their

client—just as every cleared defense counsel in a case involving classified information has the requisite need to know discoverable classified information.

We offer a final word on the government's professed security concerns. In case after case over the years, the government has made national security claims that have proven exaggerated. To cite a few famous examples, the government argued in 1971 that disclosure of the Pentagon Papers would cause grave damage to national security. *See New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam). The New York Times published the Papers, and there is no evidence that national security suffered. In 1979, the government sought to suppress Howard Morland's article, The H-Bomb Secret, claiming that publication would cause immediate and irreparable harm to national security. *See United States v. Progressive, Inc.*, 486 F. Supp. 5 (D. Wis.), *dismissed as moot*, 610 F.2d 819 (7th Cir. 1979). The Progressive published Morland's article in November 1979, and—again—there is no evidence of any harm to national security. In December 1999, the government made strident national security claims to convince a federal court to detain Dr. Wen Ho Lee under extraordinarily strict conditions for nine months. *See United States v. Lee*, 79 F. Supp. 2d 1280 (D.N.M. 1999), *aff'd mem.*, 2000 U.S. App. LEXIS 3082 (10th Cir. Feb. 29, 2000). In September 2000, following a plea bargain, Dr. Lee regained his freedom. There is no evidence that his release has caused any damage to the national security.

These examples share several common features: in each case, the government invoked national security to convince a court to depart from statutory or constitutional standards; in each case, courts initially acceded to the government's national security claims; and in each case, when the "doomsday" event actually occurred, the government's purported concerns proved unfounded. As the Fourth Circuit has observed in the First Amendment context:

> History teaches how easily the spectre of a threat to "national security" may be used to justify a wide variety of repressive government actions. A blind acceptance by the courts of the government's insistence on the need for secrecy, without notice to others, without argument, and without a statement of reasons, would impermissibly compromise the independence of the judiciary and open the door to possible abuse.

In re Washington Post Co., 807 F.2d 383, 391-92 (4th Cir. 1986).

Here, as in *Washington Post*, the government's claim of doom if § 1806(f) is interpreted in accordance with Congressional intent must be viewed skeptically. National security will no more suffer if the FISA materials are disclosed to cleared defense counsel, with all the strict and time-tested protections CIPA affords, than it will in the everyday disclosures to cleared prosecutors.[39] And if the government

[39] What can readily be seen is the effort of the intelligence agencies to resist any effort to control their province. This agency concern is not limited to defense lawyers. A telling description of the issue is set forth in former CIA lawyer John Rizzo's recent book, *Company Man: Thirty Years of Controversy and Crisis in The CIA* (Scribner 2014). In discussing the use of classified evidence in espionage cases, and the tension created between the agency and the DOJ prosecutors, Rizzo candidly acknowledges: "We tell the DOJ that we will turn cartwheels to provide our intelligence secrets necessary to get a conviction, but we are going to push back hard if we think the DOJ is going for overkill by putting sensitive information into jeopardy when it doesn't have to." *Id.* at 67. Indeed, it is of no small consequence that the Department of Justice

ultimately finds that risk unacceptable, then, as the Senate Judiciary and Intelligence Committees observed, it "must choose—either disclose the material or forego the use of the surveillance-based evidence." S. Rep. 604(I), 95th Cong., 1st Sess. 59, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960; *see* S. Rep. 701, 95th Cong., 1st Sess. 65, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4044. The Republic, or what is left of it, will survive.

D. Summary.

The "chameleon-like" word "necessary" has no "plain" meaning, and certainly not the meaning the government seeks to assign to it. Courts have interpreted the word to mean everything from "helpful" to "essential," depending on the context. The context here—particularly the legislative history of FISA and the statutory purpose to balance national security and civil liberties—points toward an intermediate meaning, such as the "substantially promote" formulation in *Butenko*, which the Senate Judiciary and Intelligence Committees endorsed.

(continued…)

Counterterrorism Section was taken out of the Criminal Division chain of command and merged into a newly created National Security Division in 2006. This move was a fundamental shift in priorities and organizational oversight. Indeed, three new sections were created "to handle the increased Foreign Intelligence Surveillance Act (FISA) workload, better coordinate FISA litigation and improve national security oversight." *See Structural Changes to Enhance Counter-Terrorism Efforts, http://www.justice.gov/911/counterterrorism.html* Needless to say, permitting intelligence agencies to dictate the responsibilities of prosecutors, defense lawyers, or this Court in a federal criminal case is a slippery slope of gargantuan proportions.

As *Butenko* suggests, application of that intermediate standard requires that the district court enjoy broad discretion to consider all relevant circumstances. The district court exercised that discretion here. After a "thorough and careful review of the FISA application and related materials," the court determined that although it is "capable" of determining the legality of the surveillance ex parte, the determination is "best made" in an adversarial proceeding. SA5. The court concluded, in other words, that adversarial proceedings will substantially promote an accurate determination of legality. Just as it was within the discretion of the district court in *Butenko* "to grant or deny Ivanov's request for disclosure and a hearing," so was it in the discretion of the district court here to make that decision.

IV. THE GOVERNMENT'S REMAINING COMPLAINTS ABOUT THE DISTRICT COURT'S ORDER ARE BASELESS.

The government offers two further complaints about the district court's order. Neither has merit, and neither shows that the court's ruling was irrational and thus an abuse of discretion. We address the government's points briefly.

A. The District Court Recited the Correct Legal Standard.

First, focusing on the district court's use of the phrase "may be necessary" in one part of its opinion, the government insists that the court applied the wrong legal standard. *E.g.*, G.Br.12, 32. In large measure, the government's complaint rests on its unduly strict interpretation of "necessary." The district court's analysis, viewed as a whole, merely recognizes that, under the circumstances of this case, an

adversarial presentation will substantially promote the accuracy of the court's determinations about the legality of the FISA surveillance.

The government is wrong for a second reason. This Court has often held, in response to similarly hypertechnical arguments of criminal defendants, that district judges are not required to "recite 'magic words'" to demonstrate their adherence to a statutory standard. *United States v. Woods*, 556 F.3d 616, 623 (7th Cir. 2009) (referring to 18 U.S.C. § 3553(a)); *see, e.g., United States v. Tyra*, 454 F.3d 686, 687 (7th Cir. 2006) (same). That principle applies equally here. The district court recognized and recited the correct "is necessary" standard under 50 U.S.C. § 1806(f). SA3-4. It is unlikely that the court forgot or chose to ignore that standard a page-and-a-half later in its opinion.[40] The issue here is not whether the court applied the proper rule—it clearly did—but whether it applied that rule in an "arbitrary" or "irrational" way. In this Court's words, the question is whether it can fairly be said that "no reasonable person could take the view of the trial court." *Dumeisi*, 424 F.3d at 574. The district court's thoughtful and considered ruling must be affirmed under that standard.

[40] To illustrate the shallowness of the government's "legal error" argument, consider Attorney General Holder's declaration and claim of privilege in this case. At page 2, the declaration avers that disclosure of the FISA materials "would harm the national security of the United States." A2. That is the correct legal standard under 50 U.S.C. § 1806(f). On the next page, however, the Attorney General asserts that such disclosure "could" harm the national security. A3. The use of "could," after recitation of the correct "would" standard, no more vitiates the declaration than the district court's use of "may be necessary," after recitation of the correct "is necessary" standard, vitiates the disclosure order.

B. The District Court Had No Obligation To Detail Its Analysis in Its Order.

Second, the government insists that the district court had to specify a "case-specific reason" for disclosure in its order. G.Br.20, 21, 22. Not surprisingly, it cites no authority for this proposition. In fact, it is customary for courts addressing FISA and other classified information issues *not* to spell out the decision making process on the record. *See, e.g., United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010) (court is "necessarily circumspect" in its discussion of FISA materials); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) ("Given the sensitive nature of the information upon which we have relied in making this determination and the Attorney General's conclusion that disclosure of the underlying information would harm the national security, it would be improper to elaborate further."); *United States v. Isa*, 923 F.2d 1300, 1304 (8th Cir. 1991) (finding probable cause to authorize FISA surveillance; court notes that "[b]ecause of the Affidavit and Claim of Privilege filed by the Attorney General of the United States, we make no further public statement"). By alluding to its "thorough and careful review" but making no further comment, the district court provided assurances that it had fully considered the "case-specific" circumstances, but without spreading those circumstances on the record and thus damaging national security.

CONCLUSION

For the foregoing reasons, the Court should affirm the district court's order.

STATEMENT CONCERNING ORAL ARGUMENT

Appellee requests oral argument. The Court has scheduled argument for June 4, 2014.

DATED: May 2, 2014

Respectfully submitted,

/s/ Thomas Anthony Durkin
Thomas Anthony Durkin

/s/ John D. Cline
John D. Cline

/s/ Joshua G. Herman
Joshua G. Herman

Attorneys for Defendant-Appellee
ADEL DAOUD

CERTIFICATE OF COMPLIANCE PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

I certify that pursuant to Fed. R. App. P. 32(a)(7)(C) the foregoing brief is proportionately spaced, has a typeface of 14 points, and contains 10,693 words.

/s/ John D. Cline
John D. Cline

CERTIFICATE OF SERVICE

When All Case Participants Are Registered For The Appellate CM/ECF System

I hereby certify that on the 2d of May, 2014, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ John D. Cline
John D. Cline

STATUTORY APPENDIX

STATUTORY APPENDIX TABLE OF CONTENTS

50 U.S.C. § 1801

Current through PL 113-96, with gaps of 113-79 and 113-93, approved 4/3/14

§ 1801. Definitions [Caution: See prospective amendment note below.]

As used in this *title [50 USCS §§ 1801* et seq.]:

(a) ″Foreign power″ means--

(1) a foreign government or any component thereof whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) ″Agent of a foreign power″ means--

(1) any person other than a United States person, who--

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore;

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who--

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation

of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) ″International terrorism″ means activities that--

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended--

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) ″Sabotage″ means activities that involve a violation of chapter 105 of title 18, United States Code [*18 USCS §§ 2151* et seq.], or that would involve such a violation if committed against the United States.

(e) ″Foreign intelligence information″ means--

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to 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; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) ″Electronic surveillance″ means--

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under *section 2511(2)(i) of title 18, United States Code*;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio 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; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) ″Attorney General″ means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under *section 507A of title 28, United States Code*.

(h) ″Minimization procedures″, with respect to electronic surveillance, means--

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law

enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a) [*50 USCS § 1802(a)*], procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 [*50 USCS § 1805*] is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) ″United States person″ means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [*8 USCS § 1101(a)(20)*]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

(j) ″United States″, when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) ″Aggrieved person″ means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) ″Wire communication″ means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) ″Person″ means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) ″Contents″, when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) ″State″ means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(p) ″Weapon of mass destruction″ means--

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in *section 178 of title 18, United States Code*) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

History

(Oct. 25, 1978, *P.L. 95-511, Title I, § 101, 92 Stat. 1783; Dec. 3, 1999, P.L. 106-120*, Title VI, § 601, 113 Stat. 1619; Oct. 26, 2001, *P.L. 107-56*, Title X, § 1003, 115 Stat. 392; Dec. 28, 2001, *P.L. 107-108*, Title III, § 314(a)(1), (c)(2), 115 Stat. 1402, 1403; Dec. 17, 2004, *P.L. 108-458*, Title VI, Subtitle A, § 6001(a), 118 Stat. 3742; March 9, 2006, *P.L. 109-177*, Title V, § 506(a)(5), 120 Stat. 248; July 10, 2008, *P.L. 110-261*, Title I, § 110(a), 122 Stat. 2465; Oct. 7, 2010, *P.L. 111-259*, Title VIII, § 801(1), 124 Stat. 2746.)

50 U.S.C. § 1803

Current through PL 113-96, with gaps of 113-79 and 113-93, approved 4/3/14

§ 1803. Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review.

(1) The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this Act, except that no judge designated under this subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this Act which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this Act, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b).

(2) (A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 501(f) [*50 USCS § 1861(f)*] or paragraph (4) or (5) of section 702(h) [50 USCS § 1872(h)], hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that--

(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

(ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this Act to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this Act on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) Court of review; record, transmittal to Supreme Court. The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this Act. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) Expeditious conduct of proceedings; security measures for maintenance of records. Proceedings under this Act shall be conducted as expeditiously as possible. The record of proceedings under this Act, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.

(d) Tenure. Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) shall be designated for terms of three, five, and seven years.

(e) Jurisdiction and procedures for review of petitions.

(1) Three judges designated under subsection (a) who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section 501(f)(1) or 702(h)(4) [*50 USCS § 1861(f)(1)* or *1881a(h)(4)*].

(2) Not later than 60 days after the date of the enactment of the USA PATRIOT Improvement and Reauthorization Act of 2005 [enacted March 9, 2006], the court established under subsection (a) shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 501(f)(1) or 702(h)(4) [*50 USCS § 1861(f)(1)* or *1881a(h)(4)*] by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

(f) Stay of order.

(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this Act, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this Act.

(g) Establishment and transmittal of rules and procedures.

(1) The courts established pursuant to subsections (a) and (b) may establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this Act.

(2) The rules and procedures established under paragraph (1), and any modifications of such rules and procedures, shall be recorded, and shall be transmitted to the following:

(A) All of the judges on the court established pursuant to subsection (a).

(B) All of the judges on the court of review established pursuant to subsection (b).

(C) The Chief Justice of the United States.

(D) The Committee on the Judiciary of the Senate.

(E) The Select Committee on Intelligence of the Senate.

(F) The Committee on the Judiciary of the House of Representatives.

(G) The Permanent Select Committee on Intelligence of the House of Representatives.

(3) The transmissions required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(h) Compliance with orders, rules, and procedures. Nothing in this Act shall be construed to reduce or contravene the inherent authority of the court established under subsection (a) to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court.

History

(Oct. 27, 1978, *P.L. 95-511, Title I, § 103, 92 Stat. 1788; Oct. 26, 2001, P.L. 107-56*, Title II, § 208, 115 Stat. 283; Dec. 17, 2004, *P.L. 108-458*, Title I, Subtitle G, § 1071(e), 118 Stat. 3691; March 9, 2006, *P.L. 109-177*, Title I, §§ 106(f)(1), 109(d), 120 Stat. 197, 205; Aug. 5, 2007, *P.L. 110-55*, § 5(a), 121 Stat. 556; July 10, 2008, *P.L. 110-261*, Title I, § 109(a)-(b)(2)(A), (c), (d), Title IV, § 403(a)(1)(B)(ii), 122 Stat. 2464, 2465, 2474; Oct. 7, 2010, *P.L. 111-259*, Title VIII, §§ 801(2), 806(a)(2), 124 Stat. 2746, 2748.)

50 U.S.C. § 1804

Current through PL 113-96, with gaps of 113-79 and 113-93, approved 4/3/14

§ 1804. Applications for court orders

(a) Submission by Federal officer; approval of Attorney General; contents. Each application for an order approving electronic surveillance under this *title [50 USCS §§ 1801* et seq.] shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 103 [*50 USCS § 1803*]. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this *title [50 USCS §§ 1801* et seq.]. It shall include--

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) 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;

(4) a statement of the proposed minimization procedures;

(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 101(e) [*50 USCS § 1801(e)*]; and

(E) including a statement of the basis for the certification that--

(i) the information sought is the type of foreign intelligence information designated;

and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(8) a statement of the facts concerning all previous applications that have been made to any judge under this *title [50 USCS §§ 1801* et seq.] involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and

(9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this *title [50 USCS §§ 1801* et seq.] should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

(b) Additional affidavits or certifications. The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) Additional information. The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 105 [*50 USCS § 1805*].

(d) Personal review by Attorney General.

(1) (A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) an application under that subsection for a target described in section 101(b)(2) [*50 USCS § 1801(b)(2)*].

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2) (A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

History

(Oct. 25, 1978, *P.L. 95-511, Title I, § 104, 92 Stat. 1788; Dec. 27, 2000, P.L. 106-567*, Title VI, § 602(a), 114 Stat. 2851; Oct. 26, 2001, *P.L. 107-56*, Title II, § 218, 115 Stat. 291; Dec. 17, 2004, *P.L. 108-458*, Title I, Subtitle G, § 1071(e), 118 Stat. 3691; March 9, 2006, *P.L. 109-177*, Title I, § 108(a)(1), 120 Stat. 203; July 10, 2008, *P.L. 110-261*, Title I, § 104, 122 Stat. 2460; Oct. 7, 2010, *P.L. 111-259*, Title VIII, § 806(a)(2), 124 Stat. 2748.)

50 U.S.C. § 1805

Current through PL 113-96, with gaps of 113-79 and 113-93, approved 4/3/14

§ 1805. Issuance of order [Caution: See prospective amendment note below.]

(a) Necessary findings. Upon an application made pursuant to section 104 [*50 USCS § 1804*], the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--

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

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

(A) the target of the electronic surveillance is a foreign power or agent of a foreign power: *Provided,* That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the *first amendment to the Constitution of the United States*; and

(B) 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;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 101(h) [*50 USCS § 1804(h)*]; and

(4) the application which has been filed contains all statements and certifications required by section 104 [*50 USCS § 1804*] and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 104(a)(7)(E) and any other information furnished under section 104(d).

(b) Determination of probable cause. In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) Specifications and directions of orders.

(1) Specifications. An order approving an electronic surveillance under this section shall specify--

(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 104(a)(3) [*50 USCS § 1804(a)(3)*];

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

(2) Directions. An order approving an electronic surveillance under this section shall direct--

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds, based on specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(3) Special directions for certain orders. An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of--

(A) the nature and location of each new facility or place at which the electronic surveillance is directed;

(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated.

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 101(a)(1), (2), or (3) [*50 USCS § 1801(a)(1)*, (2) or (3)], for the period specified in the application or for one year,

whichever is less, and (B) an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this *title [50 USCS §§ 1801* et seq.] may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this Act for a surveillance targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 101(a) [*50 USCS § 1801(a)*], or against a foreign power as defined in section 101(a)(4) [*50 USCS § 1801(a)(4)*] that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Emergency orders.

(1) Notwithstanding any other provision of this *title [50 USCS §§ 1801* et seq.], the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General--

(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this *title [50 USCS §§ 1801* et seq.] to approve such electronic surveillance exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under section 103 [*50 USCS § 1803*] at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

(D) makes an application in accordance with this *title [50 USCS §§ 1801* et seq.] to a judge having jurisdiction under section 103 [*50 USCS § 1803*] as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this *title [50 USCS §§ 1801* et seq.] for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 103 [*50 USCS § 1803*].

(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel. Notwithstanding any other provision of this *title [50 USCS §§ 1801* et seq.], officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to--

(1) test the capability of electronic equipment, if--

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) ***Provided,*** That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if--

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of title 18, United States Code [*18 USCS §§ 2510* et seq.], or *section 705* of the Communications Act of 1934 [*47 USCS § 605*], or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if--

(A) it is not reasonable to--

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this *title [50 USCS §§ 1801* et seq.]; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(g) Retention of certifications, applications and orders. Certifications made by the Attorney General pursuant to section 102(a) [*50 USCS § 1802(a)*] and applications made and orders granted under this *title [50 USCS §§ 1801* et seq.] shall be retained for a period of at least ten years from the date of the certification or application.

(h) Bar to legal action. No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

(i) Pen registers and trap and trace devices. In any case in which the Government makes an application to a judge under this *title [50 USCS §§ 1801* et seq.] to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 402(d)(2) [*50 USCS § 1842(d)(2)*].

History

(Oct. 25, 1978, *P.L. 95-511, Title I, § 105, 92 Stat. 1790; Oct. 30. 1984, P.L. 98-549, § 6(a)(3), 98 Stat. 2804; Dec. 27, 2000, P.L. 106-567*, Title VI, § 602(b), 114 Stat. 2851; Oct. 26, 2001, *P.L. 107-56*, Title II, §§ 206, 207(a)(1), (b)(1), 225, 115 Stat. 282, 295; Dec. 28, 2001, *P.L. 107-108*, Title III, § 314(a)(2), (c)(1), 115 Stat. 1402, 1403; Nov. 2, 2002, *P.L. 107-273*, Div B, Title IV, § 4005(c), 116 Stat. 1812; Dec. 17, 2004, *P.L. 108-458*, Title I, Subtitle G, § 1071(e), 118 Stat. 3691; March 9, 2006, *P.L. 109-177*, Title I, §§ 102(b)(1), 105(a), 108(a)(2), (b), 120 Stat. 195, 203; July 10, 2008, *P.L. 110-261*, Title I, §§ 105(a), 110(c)(1), 122 Stat. 2461, 2466; Dec. 19, 2009, *P.L. 111-118*, Div B, § 1004(a), 123 Stat. 3470; Feb. 27, 2010, *P.L. 111-141*, § 1(a), *124 Stat. 37*; Oct. 7, 2010, *P.L. 111-259*, Title VIII, § 806(a)(2), 124 Stat. 2748; Feb. 25, 2011, *P.L. 112-3*, § 2(a), *125 Stat. 5*; May 26, 2011, *P.L. 112-14*, § 2(a), *125 Stat. 216*.)

50 U.S.C. § 1806

Current through PL 113-96, with gaps of 113-79 and 113-93, approved 4/3/14

§ 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 obtained 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 authorization 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 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.

(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 coordinate 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*].

History

(Oct. 25, 1978, *P.L. 95-511, Title I, § 106, 92 Stat. 1793; Oct. 26, 2001, P.L. 107-56*, Title V, § 504(a), 115 Stat. 364; Nov. 25, 2002, *P.L. 107-296*, Title VIII, Subtitle I, § 898, 116 Stat. 2258; July 10, 2008, *P.L. 110-261*, Title I, §§ 106, 110(b)(1), 122 Stat. 2462, 2466.)

UNPUBLISHED CASES
(Pursuant to Fed. R. App. P. 32.1(b))

United States v. Gowadia

United States District Court for the District of Hawaii
August 6, 2010, Decided; August 6, 2010, Filed
CR. NO. 05-00486 SOM-KSC

Reporter: 2010 U.S. Dist. LEXIS 80572

UNITED STATES OF AMERICA, Plaintiff, vs. NOSHIR S. GOWADIA, Defendant.

Prior History: *United States v. Gowadia, 2010 U.S. Dist. LEXIS 45310 (D. Haw., May 8, 2010)*

Core Terms

classified information, classify, defense counsel, agents, classification, security clearance, defense witness, notice, seal, national security, protective order, disclosure, clearance, designee, unauthorized, government attorney, prosecution team, public domain, secret

Counsel: **[*1]** FLORENCE T. NAKAKUNI #2286, United States Attorney, District of Hawaii.

ELLIOT ENOKI #1528, First Assistant U.S. Attorney.

KENNETH M. SORENSON, Assistant U.S. Attorney, Honolulu, Hawaii.

ROBERT E. WALLACE, JR., Senior Trial Attorney, United States Department of Justice, National Security Division, Counterespionage Section, Washington, DC, Attorneys for Plaintiff, UNITED STATES OF AMERICA.

Judges: Susan Oki Mollway, Chief United States District Judge.

Opinion by: Susan Oki Mollway

Opinion

AMENDED PROTECTIVE ORDER

This matter comes before the Court to amend the Joint Protective Order entered by this Court on June 6, 2006. The amended protective order updates the names of the current Court Security Officer, Air Force Security Officer designated for the defense, the Clearance Attorney, as well as the government attorneys and defense counsel assigned to this case.

Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 (2000) ("CIPA"), the Security Procedures Established Pursuant to CIPA by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA section 9), *Rules 16(d)* and *57 of the Federal Rules of Criminal Procedure*, **[*2]** the general supervisory authority of the Court, and in order to protect the national security, the following Amended Protective Order is entered:

1. The Court finds that this case will involve information that has been classified in the interest of the national security. The storage, handling and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to which requires the appropriate security clearances and special access. The purpose of this Order is to establish procedures that must be followed by counsel and the parties in this case. These procedures will apply to all pretrial, trial, post-trial and appellate matters concerning classified information and may be modified from time to time by further order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

2. Definitions. The following definitions shall apply to this Order:

a. ″Classified information″ shall mean:

(i) any document or information which has been classified by any executive agency in the interests of national security or pursuant to Executive Order 13526 or its predecessor orders, as ″CONFIDENTIAL,″ **[*3]** ″SECRET,″ ″TOP SECRET,″ or additionally controlled as ″SENSITIVE COMPARTMENTED INFORMATION″ (″SCI″), or ″SPECIAL ACCESS REQUIRED″ or any information contained in such document;

(ii) any document or information now or formerly in the possession of a private party which (A) has been derived from information from the United States government that was classified and (B) has subsequently been determined to have been classified at all relevant times by the United States pursuant to Executive Order 13526 as ″CONFIDENTIAL,″ ″SECRET,″ ″TOP SECRET,″ or additionally controlled as ″SENSITIVE COMPARTMENTED INFORMATION″ (″SCI″)or ″SPECIAL ACCESS REQUIRED;″

(iii) verbal classified information known to the Defendant or defense counsel;

(iv) any information, regardless of place of origin and including ″foreign government information,″ as that term in defined in Executive Order 13526, that could reasonably be believed to contain classified information, or that refers or relates to national security or intelligence matters;

(v) any document or information as to which the defendant or defense counsel have been notified orally or in writing that such document or information contains classified information.

b. **[*4]** ″Document″ shall mean any material containing information. The term ″document″ shall include, without limitation, written or printed matter of any kind including originals, conforming copies, non-conforming copies (e.g., a copy of an original with an added notation). The term ″document″ shall also include, without limitation, letters, reports, summaries, memoranda, notes, communications, telexes, cables, telecopies, telegrams, facsimiles, microfilms, reports, photographs, charts, graphs, maps, invoices, accountings, worksheets, bulletins, transcripts, and messages, as well as alterations, amendments, modifications and changes of any kind to the foregoing; and all recordings of information on magnetic, electronic, or optic media such as audio or video tapes, computer tapes or discs, microfiche, type-writer ribbons, films and all manner of electronic data processing storage.

c. ″Access to classified information″ means having access to, reviewing, reading, learning or otherwise coming to know in any manner classified information.

d. ″Secure Area″ means a sensitive compartmented information facility accredited by a Court Security Officer for the storage, handling and control of classified **[*5]** information.

3. Information in the public domain is ordinarily not classified. However, if classified information is reported in the press or otherwise enters the public domain, the information does not lose its classified status merely because it is in the public domain. Information reported in the press or otherwise in the public domain may be considered classified and subject to the provisions of CIPA if the information, in fact, remains classified and is confirmed by any person who has, or has had, such access to classified information and that confirmation corroborates the information in question. Accordingly, any attempt by the defense to have classified information that has been reported in the public domain confirmed or denied at trial or in any public proceeding in this case shall be governed by CIPA and all provisions of this Order.

4. All classified documents and information contained therein, shall remain classified unless

the documents bear a clear indication that they have been declassified by the agency or department that originated the document or information contained therein (″originating agency″).

5. In accordance with the provisions of CIPA and the Security Procedures **[*6]** promulgated by the Chief Justice of the United States pursuant to that Act, this Court designates Joan B. Kennedy as Court Security Officer and Michael Macisso, Christine Gunning, Dan Hartenstine, W.S. Slade, Miguel Ferrer and Maura Peterson as alternate Court Security Officers for this case, for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information or documents that have been made available to defendant Noshir S. Gowadia as a result of his prior relationship with the government, or will be made available to the defense in connection with this case. Defense counsel shall seek guidance from the Court Security Officer with regard to appropriate storage, handling, transmittal, and use of classified information.

6. The Court has been advised that the Assistant United States Attorneys assigned to this case, Kenneth M. Sorenson and Elliot Enoki, and Department of Justice attorneys Robert E. Wallace, Jr. and John J. Dion have the requisite security clearances allowing them to have access to the classified documents and information that relate to this case. Any references to government attorneys as used in this Order refer **[*7]** only to the attorneys listed in this paragraph.

7. The Defendant, his counsel, and counsels' approved agents, consultants and employees, shall be given access to classified national security documents and information as required by the government's discovery obligations and in accordance with the terms of this Protective Order, and any other orders pursuant to CIPA, and upon receipt of appropriate security clearances and required access. Any additional person whose assistance the defense reasonably requires may only have access to classified information in this case after obtaining from a designated Air Force Security Officer who is to be ″walled off″ from all attorneys and investigators on the prosecution ″team″ (the ″Air Force Security Officer″), with prior notice to the government, an approval for access to the required level of classification on a need to know basis, and after satisfying the other requirements described in this Order for access to classified information. The Air Force Security Officer designated to assist the defendant is Laurie Graber of the Air Force Office of Special Investigations. Any such potential witness will be approved for or confirmed to have access to **[*8]** the required level of classification and to the specific special access program relevant to this case, and will be further instructed by the designated Air Force Security Officer to limit discussion with the defense to only those matters which are within the specific special access program. Whenever the defense seeks to conceal the identity of such a potential witness or expert from the prosecution team, it must identify the proposed witness and the reasons for the desire to keep his or her identify secret to a designated government attorney who is to be ″walled off″ from all attorneys and investigators on the prosecution team (the ″Clearance Counsel″). Mary Ruppert of the Department of Justice shall serve as the Clearance Counsel. If Clearance Counsel believes the prosecution team should receive notice of the identity of the proposed witness, Clearance Counsel will move the Court, with notice to the defense, for such disclosure and represent the government in any hearing on the matter. Any rejected request for such approval may be appealed to the Court, with notice to be provided to the Air Force Security Officer and either the government or Clearance Counsel. If the defense determines **[*9]** that access to classified information in another special access program is necessary to its defense of Mr. Gowadia, it must move the Court, with notice to the Air Force Security Officer and either the government or Clearance Counsel, for an order granting such access. The substitution, departure, or removal from this case of defense

counsel or anyone associated with the defense as an agent, consultant, employee or witness or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

8. The Court Security Officer shall arrange for an appropriately approved secure area for the use of defense counsel, and their agents, consultants and employees. The Court Security Officer shall establish procedures to assure that the secure area is accessible during business hours to defense counsel, their agents, consultants and employees, and authorized witnesses accompanied by defense counsel, and at other times upon reasonable request as approved by the Court Security Officer. The secure area shall contain a separate working area for defense counsel and will be outfitted with any secure office equipment requested **[*10]** by the defense that is reasonable and necessary to the preparation of the defense. The Court Security Officer, in consultation with defense counsel, shall establish procedures to assure that the secure area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No classified documents may be removed from the secure area unless so authorized by the Court Security Officer with notice provided to the Court. The Court Security Officer shall not reveal to the government the content of any conversations he or she may hear among the defense, nor reveal the nature of the documents being reviewed or the work being generated. The presence of the Court Security Officer shall not operate to render inapplicable the attorney-client privilege.

9. Filing of Papers by Defendant. Any pleading or other document filed by the defendant shall be filed under seal with the Court through the Court Security Officer or his or her designee, and shall be marked, ″Filed in Camera and Under Seal with the Court Security Officer,″ unless defense counsel has obtained permission from the Court Security Officer, specific to a particular, non-substantive pleading **[*11]** or document (e.g., motions for extensions of time, continuances, scheduling matters, etc.) which does not contain information that is or may be classified or require filing under seal, to file the document not under seal. The time of physical submission to the Court Security Officer or a designee shall be considered the date and time of filing. The Court Security Officer shall submit the document to the designated Air Force Original Classification Authority who is instructed not to disclose to all attorneys and investigators on the prosecution ″team″ all communications and correspondence related to any requests from defendant or his counsel for classification determinations. The designated Air Force Original Classification Authority shall promptly examine the pleading or document and, in consultation with representatives of the appropriate agencies, determine whether the pleading or document contains classified information. If the designated Air Force Original Classification Authority determines that the pleading or document contains classified information, the Court Security Officer and the designated Air Force Original Classification Authority shall ensure that the document is marked **[*12]** with the appropriate classification marking and remains under seal. All papers filed by the Defendant that do not contain classified information shall be immediately unsealed by the Court Security Officer and placed in the public record. The Court Security Officer or a designee shall immediately deliver under seal to the Court and counsel for the United States any pleading or document to be filed by the defendant that contains classified information; the Court shall then direct the clerk to enter on the docket sheet the title of the pleading or document, the date it was filed, and the fact that it has been filed under seal with the Court Security Officer or a designee.

10. Filing of Papers by the United States. Any pleadings or documents filed by the United States that contain classified information shall be filed under seal with the Court through the Court Security Officer or his or her designee and such

designated Air Force Original Classification Authority pleadings shall be marked, "Filed in Camera and Under Seal with the Court Security Officer." The date and time of physical submission of such pleadings to the Court Security Officer or a designee shall be considered the date and **[*13]** time of filing.

11. The Court Security Officer shall maintain a separate sealed record for those materials which are classified. The Court Security Officer shall be responsible for the maintaining of the secured records for purposes of later proceedings or appeal.

12. Protection of Classified Information. The Court finds that to protect the classified information involved in this case, individuals other than counsel for the United States, appropriately cleared Department of Justice employees, and personnel of the originating agency, can obtain access to classified documents and information only after having been granted a security clearance by the Department of Justice through the Court Security Officer, and with permission of the Court. No person except counsel for the Defendant, and the agents, consultants and employees of counsel for the Defendant or defense witnesses, upon receipt of appropriate security clearances and special access, shall have access to the classified information involved in this case. Moreover, no counsel for the Defendant, and no agents, consultants and employees of counsel for the Defendant, nor any defense witnesses shall have access to any classified information **[*14]** in this case unless that person shall first have:

(a) received from the Court Security Officer the appropriate security clearances and special access required for the level of the classified information involved in this litigation; and

(b) signed the Memorandum of Understanding in the form attached hereto agreeing to comply with the terms of this Order. The signed Memorandum of Understanding shall be filed with the Court Security Officer. The substitution, departure or removal for any reason from this case of counsel for the defense or anyone associated with the defense as an employee or witness or otherwise shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

Before any person other than counsel for the United States, appropriately cleared Department of Justice employees, and personnel of the originating agency, is permitted by the Court to inspect and review classified national security information, he or she must also sign the attached Memorandum of Understanding.

13. Access to Classified Information. In the interest of the national security, the defendant may be excluded from access to certain **[*15]** classified information. Counsel for the Defendant, and any agents, consultants, and employees of counsel for the Defendant and any defense witnesses accompanied by counsel for the Defendant shall have access to classified information only as follows:

a. All classified information produced by the government to defense counsel in discovery or otherwise, and all classified information possessed, created or maintained by the defense, shall be stored, maintained and used only in the secure area established by the Court Security Officer.

b. Counsel for the defendant, and any agents, consultants, and employees of counsel for the Defendant shall have free access to the classified information made available to them in the secure area established by the Court Security Officer and shall be allowed to take notes and prepare documents with respect to those materials.

c. No person, including counsel for the defendant, and any agents, consultants, or employees of counsel for the defendant or defense witnesses, shall copy or reproduce any classified information in any manner or form,

except with the approval of the Court Security Officer or in accordance with the procedures established by the Court Security **[*16]** Officer for the operation of the secure area.

d. All documents prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in a secure area on word processing equipment approved by the Court Security Officer. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits) containing classified information shall be maintained in the secure area unless and until the Court Security Officer determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the United States or any other party.

e. Counsel for the Defendant, and any agents, consultants, and employees of counsel for the Defendant shall discuss classified information only within the secure area or in an area authorized by the Court Security Officer.

f. The defense shall not disclose, without prior approval of the Air Force Security Officer or the Court, the contents of any classified documents or information to any person not named in this Order except the **[*17]** Court, Court personnel and the attorneys for the United States identified by the Court Security Officer as having the appropriate clearances, special access and the need to know. Any rejected request for such disclosure may be appealed to the Court, with notice to be provided to the Air Force Security Officer and either the government or Clearance Counsel. Any person approved by the Air Force Security Officer or the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearances and special access, to sign and submit to the Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, the Air Force Security Officer and Court Security Officer shall promptly seek to obtain security clearances and special access for them at the request of defense counsel. Any such person will be instructed further by the designated Air Force Security Officer to limit discussion with the defense to only those matters which are within the specific special access program.

g. The Defendant, **[*18]** counsel for the Defendant, and any agents, consultants, and employees of counsel for the Defendant, defense witnesses, the government and government witnesses shall not discuss classified information over any standard commercial telephone instrument or inter-office communication systems, including but not limited to the Internet, or in the presence of any person who has not been granted access by the Court to classified information.

h. Any documents written by the defense that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

i. If counsel for the government advise defense counsel that certain classified information or documents may not be disclosed to the Defendant, then defense counsel, and any agents, consultants, and employees of defense counsel, and defense witnesses shall not disclose such information or documents to the Defendant without prior concurrence of counsel for the government or, absent such concurrence, approval of the Court. Counsel for the government shall be given an opportunity to be heard in response **[*19]** to any defense request for disclosure to the defendant of such classified information.

14. Classified Information in the Defendant's Possession Prior to the Institution of this Case. The Court has been advised by the government

that the defendant may be in possession of classified information made available to him as a result of his previous associations with the government. Furthermore, as set forth in the government's Motion for Protective Order, it is clear that the defendant has a continuing contractual obligation to the government not to disclose to any unauthorized person classified information that he possesses as a result of such previous employment. The government is entitled to enforce its agreements to maintain the confidentiality of classified information. Consequently, pursuant to federal common law and the ordinary principles of contract law, the defendant is hereby enjoined from breaching the terms of the secrecy agreements to which he has subscribed throughout his employment as a government contractor, an exemplar of which is appended hereto and expressly incorporated herein. Specifically, the defendant is prohibited from any future violations of the above-referenced **[*20]** secrecy agreements, and, in particular, is enjoined from disclosing any classified information to any unauthorized person during the pendency of this Order. Nothing in this Order shall be construed as a limitation on the government in filing additional criminal charges against the defendant in the event of an unauthorized disclosure of classified information.

15. Classified Information Procedures Act. Procedures for the public disclosure of classified information by the defense shall be those established in sections 5 and 6 of CIPA. No classified information may be disclosed by the defense except:

a. to the Court, court personnel and government attorneys and their agents and employees identified by the Court Security Officer or a designee as holding proper security clearances and approvals for special access to classified information;

b. to representatives of the agency or department originating the classified information who have been identified by the Court Security Officer as holding proper security clearances and having the need to know the classified information;

c. in accordance with the procedures of CIPA and the procedures established by the Court Security Officer; or

d. to persons **[*21]** who have been authorized to have access to classified information pursuant to this Order or to CIPA. To facilitate the defense in its filing of notices as required under Section 5 of CIPA, the Court Security Officer shall make arrangements with the designated Air Force Original Classification Authority and other representatives of the appropriate Agencies for a determination of the classification level, if any, of materials or information either within the possession of the defense or about which the defense has knowledge and which the defense intends to use in any way at any pretrial proceeding or at trial. Nothing submitted by the defense to the Court Security Officer or a designee pursuant to this paragraph shall be made available to counsel for the United States unless so ordered by the Court, or so designated by the defense. Any and all of these items which are classified shall be listed in defendant's Section 5 notice.

16. The defense may not contact any employee of any government intelligence agency without making prior arrangements with a government attorney, unless the defense files a motion with the Court (which may be ex parte at the discretion of defense counsel), to authorize **[*22]** such contact, provides the government notice of such motion, and obtains a court order authorizing that contact. This is required because the identities of the government intelligence employees may be classified, and formal arrangements may be required to protect the classified information which may be the subject of discussion by the parties.

17. Any unauthorized disclosure of classified information may constitute violations of United States criminal laws. In addition, any violation of the terms of this Order shall be brought

immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention or negligent handling of classified documents or information could cause serious damage, and in some cases exceptionally grave damage to the national security of the United States or may be used to the advantage of a foreign nation against the interests of the United States. This Protective Order is to ensure that those **[*23]** authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the originating agency and in conformity with this Order.

18. All classified documents and information which counsel for the defendant, and any agents, consultants, and employees of counsel for the defendant or defense witnesses have access to in this case are now and will remain the property of the United States. Upon demand of the Court Security Officer, these persons shall return to the Court Security Officer, all classified information in their possession obtained through discovery from the government in this case, or for which they are responsible because of access to classified information. The notes, summaries and other documents prepared by the defense that do or may contain classified information shall remain at all times in the custody of the Court Security Officer for the duration of the case. At the conclusion of this case, all such notes, summaries and other documents are to be destroyed by the Court Security Officer in the presence of defense counsel.

19. No admission made by the defendant **[*24]** or defense counsel during the pretrial conference may be used against the defendant unless it is in writing and signed by the defendant. CIPA Section 2.

20. A copy of this Order shall be issued forthwith to defense counsel who shall be responsible for advising the Defendant, and any agents, consultants, and employees of counsel for the defendant, and defense witnesses of the contents of this Order. Counsel for the defendant, each agent, consultant, and employee of counsel for the defendant and defense witness who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 12 of this Order, and counsel for the defendant shall file executed originals of such documents with the Court Security Officer who shall serve an executed copy of the original upon the United States. The execution and filing of the Memorandum of Understanding is a condition precedent for counsel for the defendant, any employee of counsel for the defendant, and any defense witness to have access to classified information.

IT IS SO ORDERED.

DATED: Honolulu, Hawaii, August 6, 2010.

/s/ Susan Oki Mollway

Susan Oki Mollway

Chief United States District Judge

MEMORANDUM **[*25]** OF UNDERSTANDING

1. I, %y(13)6D, understand that I may be the recipient of information and documents that concern or implicate the national security of the United States and belong to the United States, and that such documents and information are classified according to security standards set by the United States government.

2. I agree that I shall never divulge, publish or reveal, either by word, conduct or other means, such classified information and documents unless specifically authorized in writing to do so by an authorized representative of the United States government, or as required by the Classified Information Procedures Act, or as otherwise ordered by the Court.

3. I understand this agreement will remain binding upon me after the conclusion of the proceedings in United States v. Noshir S. Gowadia, Cr. No. 05-00486 SOM-KSC, and any subsequent related proceedings.

4. I have received, read and understood the Protective Order entered by the United States District Court for the District of Hawaii in the above case, and I agree to comply with the provisions thereof.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed **[*26]** this %y(5)6D day of %y(5)6D, 2010, at %y(8)6D.

Witnessed by

JOAN B. KENNEDY

Court Security Officer

United States v. Wen Ho Lee

United States Court of Appeals for the Tenth Circuit
February 29, 2000, Filed
No. 00-2002

Reporter: 2000 U.S. App. LEXIS 3082; 2000 Colo. J. C.A.R. 1175

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. WEN HO LEE, Defendant-Appellant.

Notice: [*1] RULES OF THE TENTH CIRCUIT COURT OF APPEALS MAY LIMIT CITATION TO UNPUBLISHED OPINIONS. PLEASE REFER TO THE RULES OF THE UNITED STATES COURT OF APPEALS FOR THIS CIRCUIT.

Subsequent History: Reported in Table Case Format at: *2000 U.S. App. LEXIS 10821*.

Prior History: (D. N.M.). (D.C. No. CR-99-1417-JC).

Disposition: AFFIRMED substantially for the reasons stated in the district court's detailed opinion dated December 30, 1999. The appellee's unopposed motion to supplement the record granted.

Core Terms

tape, district court, detain, classify, adverse inference, destroy, weapon

Case Summary

Procedural Posture

Defendant appealed order of United States District Court for District of New Mexico which denied motion for revocation of pre-trial detention order issued under Bail Reform Act, *18 U.S.C.S. § 3141 et seq.*, on ground that defendant was subject to life imprisonment and presented substantial danger to nation if released.

Overview

Defendant nuclear physicist was indicted on numerous counts relating to defendant's alleged transfer of classified computer files containing data on nuclear weapons research, design, and construction to an unsecured computer system and then to computer tapes, and defendant sought release from pretrial detention. The court held that, under the Bail Reform Act, *18 U.S.C.S. § 3141 et seq.*, defendant was properly denied bail because he was charged with offenses punishable by life imprisonment and his release, regardless of any conditions, would endanger the community. The applicability of the statute was not limited to situations involving physical violence, and defendant's failure to account for missing computer tapes presented a potentially catastrophic risk to the safety of the nation. Defendant had the ability to communicate the location of the missing tapes or their contents which contained all the information necessary to design, build, operate, and evaluate a complete portfolio of thermonuclear weapons.

Outcome

Order was affirmed; bail was properly denied because defendant was a prisoner subject to life imprisonment and defendant's failure to account for missing computer tapes containing classified thermonuclear weapons construction information constituted a potentially catastrophic risk to national security if defendant were released to dispense or use the information.

LexisNexis® Headnotes

Criminal Law & Procedure > Preliminary Proceedings > Bail > General Overview

Criminal Law & Procedure > Preliminary Proceedings > Bail > Conditions of Release

Criminal Law & Procedure > Preliminary Proceedings > Bail > Dangerousness

Criminal Law & Procedure > Preliminary Proceedings > Bail > Denial of Bail

Criminal Law & Procedure > Preliminary Proceedings > Bail > Hearings

Criminal Law & Procedure > Postconviction Proceedings > Imprisonment

HN1 Under the Bail Reform Act, *18 U.S.C.S. § 3141 et seq.*, a defendant charged with an offense punishable by life imprisonment may be denied bail if, after a hearing, the government demonstrates by clear and convincing evidence that no condition or combination of release conditions will reasonably assure the safety of any other person and the community. *18 U.S.C.S. §§ 3142(e)*, *(f)(1)(B)*.

Criminal Law & Procedure > Preliminary Proceedings > Bail > Dangerousness

HN2 In determining whether the pre-trial release of a defendant would endanger the community, the court must consider the nature and circumstances of the crimes charged; the weight of the government's evidence; the history and characteristics of the defendant; and the nature and seriousness of the danger posed by the person's release. *18 U.S.C.S. § 3142(g)*.

Civil Procedure > Appeals > Standards of Review > Clearly Erroneous Review

Civil Procedure > Appeals > Standards of Review > De Novo Review

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Findings of Fact

HN3 The appellate court reviews the district court's determination of mixed questions of law and fact concerning a detention decision de novo, while accepting its findings of historical fact in support of the decision unless they are clearly erroneous.

Counsel: For UNITED STATES OF AMERICA, Plaintiff - Appellee: Robert J. Gorence, John J. Kelly, U.S. Attorney, Paula Burnett, Asst. U.S. Attorney, Office of the United States Attorney, District of New Mexico, Albuquerque, NM. Laura Fashing, Office of the US Attorney, Albuquerque, NM.

For WEN HO LEE, Defendant - Appellant: Nancy Hollander, John D. Cline, Freedman, Boyd, Daniels, Hollander, Goldberg & Cline, Albuquerque, NM. Mark Holscher, O'Melveny & Myers LLP, Los Angeles, CA.

Judges: Before TACHA, BRISCOE, and MURPHY, Circuit Judges.

Opinion

ORDER AND JUDGMENT *

[*2] After examining the briefs and appellate record, this panel has determined unanimously that oral argument would not materially assist the determination of this appeal. *See Fed. R. App. P. 34(a)(2)*; *10th Cir. R. 34.1(G)*. The case is therefore ordered submitted without oral argument.

Defendant Wen Ho Lee appeals from a district court order denying his motion for revocation of the magistrate judge's pretrial detention order. Lee, a former nuclear physicist at Los Alamos National Laboratory (LANL), was indicted on fifty-nine counts of violating the Atomic Energy Act, *42 U.S.C. § 2275* (receipt of restricted data) and *42 U.S.C. § 2276* (tampering with restricted data), and the Espionage Act, *18 U.S.C. § 793* (gathering, transmitting or losing defense information). He faces a maximum sentence of life imprisonment on these charges.

HN1 Under the Bail Reform Act, *18 U.S.C. §§ 3141-51*, a defendant charged with an offense punishable by life imprisonment may be denied bail if, after a hearing, the government

* This order and judgment is not binding precedent, except under the doctrines of law of the case, res judicata, and collateral estoppel. The court generally disfavors the citation of orders and judgments; nevertheless, an order and judgment may be cited under the terms and conditions of 10th Cir. R. 36.3.

demonstrates by clear and convincing evidence that "no condition or combination of [release] **[*3]** conditions will reasonably assure . . . the safety of any other person and the community." *18 U.S.C. §§ 3142(e)*, *(f)(1)(B)*. ***HN2*** In determining whether the release of a defendant would endanger the community, the court must consider the nature and circumstances of the crimes charged; the weight of the government's evidence; the history and characteristics of the defendant; and the nature and seriousness of the danger posed by the person's release. *18 U.S.C. § 3142(g)*.

The magistrate judge ordered Lee detained on the ground that Lee posed a "clear and present danger to the national security of the United States." Appellant's App. at 320. Following a three-day detention hearing, the district court [1] ordered Lee's continued detention. In a detailed nineteen-page order, the district court found that the government had shown by clear and convincing evidence that no combination of conditions of release would reasonably assure the safety of the community or the nation. *See United States v. Lee, 79 F. Supp. 2d 1280, 1999 WL 1279142 (D.N.M. 1999)*. ***HN3*** We review the district court's determination of mixed questions of law and fact **[*4]** concerning the detention decision *de novo*, while accepting its findings of historical fact in support of the decision unless they are clearly erroneous. *See United States v. Kinslow, 105 F.3d 555, 557 (10th Cir. 1997)*. We affirm.

Lee is charged with "downpartitioning" nineteen computer files containing 806 megabytes of classified and confidential restricted data relating to nuclear weapons research, design, and construction from secure, separately partitioned, classified computer networks at LANL, and transferring the files to a separate, unsecure computer system. [2] Lee is charged with then downloading seventeen of these classified computer files from the unsecure computer network to nine portable, magnetic computer tapes, and with downloading a classified nuclear weapons design code and its auxiliary libraries and utilities codes directly from **[*5]** the secured computer network to a tenth portable computer tape. Investigators located some of the portable tapes in Lee's desk at LANL in March 1999, after he had been terminated from LANL because of an unrelated security breach.

Seven of the portable computer tapes, containing most of the 806 megabytes of classified data, remain unaccounted for. The government presented evidence that the missing tapes contain all of the information necessary to design, build, operate, and evaluate a complete portfolio of thermonuclear weapons, from very simple, easily manufactured weapons, to the most complex thermonuclear weapons the United States is capable of designing. Experts testified that if these tapes fell into the wrong hands, it would "change the strategic **[*6]** global balance," and that the risk "represents the gravest possible security risk to the United States." Appellant's App. at 182, 602.

The district court found that "Lee's release from custody at this time poses a danger to the United States because of the risk that [he] will find a way to, and will be inclined to, reveal to unauthorized persons the location of the seven missing tapes or to assist an unauthorized possessor in understanding and utilizing the information contained in the tapes." *Lee*, 1999 WL 1279142, at *8. The district court found that the nature of the offenses Lee is alleged to have committed are "quite serious and of grave concern to national security." *Id.* at *5. The district court also found that the circumstances under which Lee is alleged to have acted are

---

[1] The Honorable James A. Parker presided over the detention hearing because the district court judge to whom the case was assigned was unavailable.

[2] 806 megabytes of data is equal to approximately 806 reams of paper. The computer forensic data showed that it took 70 days over a two-year period to transfer the huge volume of classified files from the classified computer system to the unsecured, open computer.

″deeply troubling″ and ″highly suspicious.″ *See id.* at *5, *7. These findings are not clearly erroneous. *See Kinslow, 105 F.3d at 557*.

The ″potentially catastrophic″ risk to the safety of the community, indeed the nation, presented by Lee's ability to communicate information about the location of the missing tapes or their contents if he is released pending **[*7]** trial, *Lee*, 1999 WL 1279142, at *9, is unprecedented, but nevertheless, within the boundaries of the Bail Reform Act. In adopting the Bail Reform Act, Congress specifically recognized that the ″concern about safety [under the Bail Reform Act should] be given a broader construction than merely danger of harm involving physical violence.″ S. Rep. No. 225, 98th Cong., 2d Sess., at 13 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3182, 3195; *see also United States v. Cook, 880 F.2d 1158, 1161 (10th Cir. 1989)*; *United States v. King, 849 F.2d 485, 487 n.2 (11th Cir. 1988)* (″The term 'dangerousness' as used in the Bail Reform Act of 1984, has a much broader construction than might commonly be understood in everyday parlance.″). Congress recognized that the concept of danger under *§ 3142* could be ″extended to nonphysical harms such as corrupting a union.″ 1984 U.S.C.C.A.N. at 3195-96. We can conceive of few greater threats to the safety of the community than the risks presented in this case.

Lee contends that his release does not pose a risk to the community because he destroyed the missing computer tapes. In support of this claim, however, **[*8]** he presented only a ″broad, non-specific″ representation in a letter he signed when he was fired stating generally that he had destroyed all classified materials in his possession. *Lee*, 1999 WL 1279142, at *8. The district court found that Lee presented insufficient evidence for it to conclude that the tapes had been destroyed. *See id.* This factual finding is not clearly erroneous.

Lee argues that the district court violated his *Fifth Amendment* rights against self-incrimination by drawing an adverse inference from his failure to present sworn testimony or otherwise to provide more specific evidence indicating he destroyed the missing tapes. *See id.* at *8, *9. Lee relies upon *Mitchell v. United States, 526 U.S. 314, 119 S. Ct. 1307, 1316, 143 L. Ed. 2d 424 (1999)*, in which the Supreme Court recently held that a defendant who has pleaded guilty does not waive his right to remain silent at his sentencing hearing and that the sentencing judge may not draw an adverse inference from his silence. Lee argues from this ruling that the district court erred in drawing a negative inference from his failure to present sworn testimony that he destroyed **[*9]** the missing tapes.

Lee cites us no authority applying a no-adverse inference rule to *§ 3142* detention hearings, nor are we aware of any such precedent. We decline to extend *Mitchell's* adverse inference rule to the circumstances in this case. Even assuming that the *Mitchell* adverse inference rule did apply to *§ 3142* detention hearings and that the district court's comments would be construed as an adverse inference on Lee's failure to testify, any error would be clearly harmless. The court's comment on Lee's silence was merely cumulative of the court's overall assessment of the evidence in the record concerning Lee's purported destruction of the tapes. *See Chapman v. California, 386 U.S. 18, 22, 17 L. Ed. 2d 705, 87 S. Ct. 824 (1967)*.

After an independent review of the record, we conclude that the district court properly analyzed the relevant factors under the Bail Reform Act and correctly determined that the government met its burden of establishing by clear and convincing evidence that there are no conditions or ″combination of conditions of release that will reasonably assure the safety of any other person and the community or the nation.″ *Lee*, 1999 WL 1279142, **[*10]** at *9. We AFFIRM substantially for the reasons stated in the district court's detailed opinion dated December 30, 1999. The appellee's unopposed motion to supplement the record is granted.

ENTERED FOR THE COURT

PER CURIAM