No. 14-1284

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, No. 1:12-cv-00723
The Honorable Judge Sharon Johnson Coleman

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLEE AND URGING AFFIRMANCE

Patrick Toomey
Brett Max Kaufman
Jameel Jaffer
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: 212-549-2500
ptoomey@aclu.org

Matthew R. Segal
Counsel of Record
Jessie J. Rossman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS
211 Congress Street, 3d Floor
Boston, MA 02110
Tel: 617-482-3170
msegal@aclum.org

Harvey Grossman
ROGER BALDWIN FOUNDATION OF ACLU, INC.
180 N. Michigan Ave., Suite 2300
Chicago, IL 60601
Tel: 312-201-9740
hgrossman@aclu-il.org

Hanni Fakhoury
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415-436-9333
hanni@eff.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Federal Statutes

Other

STATEMENT OF *AMICI CURIAE*

Amici are advocacy organizations with a "unique . . . perspective" on, and extensive experience with, cases involving the Foreign Intelligence Surveillance Act ("FISA"). *See Ryan v. CFTC*, 125 F.3d 1062, 1063 (7th Cir. 1997).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with over 500,000 members, and the ACLU of Illinois is one of its state affiliates. The ACLU defends the principles embodied in the Constitution and our nation's civil rights laws, and it has participated directly and as *amicus* in cases concerning FISA. *E.g.*, *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138 (2013); *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo.).

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization working to protect innovation, free speech, and privacy in the online world. With more than 30,000 dues-paying members nationwide, including 804 donors in Illinois and 3,918 Illinois-based subscribers to its weekly e-mail newsletter, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. EFF therefore has therefore participated, either directly or as *amicus*, in FISA cases. *E.g.*, *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011); *First Unitarian Church of L.A. v. NSA*, No. 13-cv-03287 (N.D. Cal. filed July 16, 2013); *In re NSA Telecomm. Records Litig.*, 671 F.3d 881 (9th

Cir. 2011); *Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d 845 (9th Cir. 2012) (amicus).

This brief is accompanied by a motion for leave to file it. No party's counsel authored this brief in whole or in part. With the exception of amici's counsel, no one, including any party or party's counsel, contributed money that was intended to fund preparing or submitting this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Foreign Intelligence Surveillance Act of 1978 reflects Congress's judgment that identifying and monitoring foreign threats can be accomplished without compromising civil liberties. FISA therefore authorizes courts to order disclosure of classified materials, when "necessary," to the targets of FISA surveillance. Confronted by revelations that inaccuracies have plagued other FISA cases, and by confusion about the facts of this case, the district court here issued a limited disclosure order. This appeal arises from the government's view that, despite these complex circumstances, this single disclosure order in 36 years is one too many.

FISA's enactment followed the Church Committee's investigation into wrongdoing by intelligence agencies. *Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II)*, S. Rep. No. 94-755, at v (1976). The agencies had "violated specific statutory prohibitions," "infringed . . . constitutional rights," and "intentionally

disregarded" statutory restrictions. *Id.* at 137. In response, Congress passed FISA to regulate the government's ability to conduct electronic surveillance and physical searches undertaken to protect national security. FISA created the Foreign Intelligence Surveillance Court ("FISC"), which can grant or deny government applications for surveillance and physical searches. 50 U.S.C. §§ 1803(a), 1822(c). Traditional FISA orders require "probable cause to believe that the target . . . is a foreign power or an agent of a foreign power." *Id.* §§ 1805(a)(2), 1824(a)(2). In 2008, however, Congress enacted the FISA Amendments Act ("FAA"), which authorizes certain surveillance that is not based on probable cause or individualized suspicion. 50 U.S.C. § 1881a. Under that authority and others, the FISC's role has expanded and grown more challenging; it now approves broad surveillance programs rather than simply specific surveillance targets.

Persons "aggrieved" by FISA orders can challenge them in court. The government must notify an aggrieved person when it plans to use or disclose at trial "any information obtained or derived from" a FISA order. *Id.* §§ 1806(c), 1825(e). The aggrieved person can then move to suppress evidence acquired "unlawfully" or "not . . . in conformity with" the FISA order. *Id.* §§ 1806(e), 1825(f). If the Attorney General avers that disclosure or an adversary hearing would harm national security, the court reviews the FISA materials *in camera* and *ex parte*. After that review, the court may order disclosure to the ag-

grieved person "where such disclosure is necessary to make an accurate determination of the legality of the" FISA order. 50 U.S.C. §§ 1806(f), 1825(g).

In this case, the government notified appellee Adel Daoud that it intends to offer, or otherwise use or disclose, evidence obtained or derived from FISA surveillance. On January 29, 2014, the district court ordered disclosure of FISA materials to Daoud's cleared counsel. SA 4–5. The court did so only after acknowledging § 1806(f)'s necessity standard, conducting a "thorough and careful" review of the FISA materials, and finding that disclosure "may be necessary" to accurately assess the legality of the FISA order in this case. SA 3–5.

Yet the government argues that the district court abused its discretion because this case is not so "extraordinary" as to justify the nation's "first" FISA disclosure order. Gov't Op. Br. 19, 32. But, of course, this is the government's argument in every disclosure case; for years, it has urged courts to follow an "unbroken rule" of non-disclosure.[1] This appeal to inertia is wrong for two reasons, one about FISA generally and one about this case specifically.

---

[1] Gov't Amended Unclassified Mem., *United States v. Kashmiri*, No. 1:09cr00830, 2010 WL 5641588, at *3, *10, *17 (N.D. Ill. June 24, 2010); Gov't Unclassified *Ex Parte* Mem., *United States v. Gowadia*, No. 05-00486, 2008 WL 7994833, at *19 (D. Haw. Dec. 16, 2008); *see also* Gov't Unclassified Br., *United States v. Squillacote*, Nos. 99-4088, 99-4089, 1999 WL 33618066, at *76 (4th Cir. Oct. 8, 1999) ("There was no reason for Judge Hilton to be the first judge in history to order disclosure of the FISA applications to the defense."); Gov't Redacted Mem., *United States v. Abu-Jihaad*, No. 3:07cr57, 2007 WL 4961129, at *22, *50–51 (D. Conn. Dec. 21, 2007)

First, warning a court against becoming an outlier is no substitute for statutory interpretation. FISA's text, structure, and legislative history all reject a rule of categorical secrecy. Instead, FISA permits disclosure even when the executive branch asserts that disclosure would harm national security, because it is rooted in a statutory scheme designed to assure meaningful judicial review of FISA orders. Although the "necessity" standard makes *in camera*, *ex parte* review a default first step, the disclosure standard is met in cases where, for any reason, a district court might reasonably lack certainty about a FISA order's legality.

Second, the context here supports the district court's ruling that this is such a case. The court's ruling followed revelations—in newly declassified FISC opinions and in reports about *Clapper v. Amnesty International*—that courts have labored under misapprehensions about the government's surveillance activities and legal theories. The order also followed public debate—arising from comments by Senator Dianne Feinstein—about whether the investigation of Daoud involved the FAA, a statute whose constitutionality has yet to be adjudicated by any federal court. Even if the district court accepted the government's representation that it does not intend to use FAA-derived

---

("there is nothing extraordinary about the FISA collection ordered in this case that would justify this case becoming the first 'exception' to the rule"); Gov't Mem., *United States v. Hassoun*, No. 04-60001, 2007 WL 1068127, at *15–16 (S.D. Fla. Apr. 4, 2007) (nearly verbatim); R.73 at 19, 20 (nearly verbatim).

material against Daoud, the recent revelations and public controversy could have led the court to conclude that shielding the FISA materials from defense counsel could cause it to miss something important.

The context for this case directly implicates Congress's view that, while *in camera* review would be a default, disclosure would be necessary in some cases. FISA's disclosure provisions are not ornamental, and the district court's decision to invoke them in this case was not an abuse of discretion.

ARGUMENT

I. FISA's text, structure, and legislative history favor disclosure of surveillance materials in complex cases.

FISA's necessity standard anticipates that disclosure will be the exception rather than the rule.[2] But it is decidedly not a "one-in-a-million" standard. *See* Gov't Op. Br. 19 (citing *In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 203 (7th Cir. 2003)).[3] The basic tools of statutory interpretation—text, structure, and legislative history—refute the government's narrow interpretation of FISA's disclosure provisions. *Cf. Fed. Aviation Admin. v. Cooper*, 132 S. Ct. 1441, 1456 (2012). The government's view

[2] *See United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011); *United States v. Isa,* 923 F.2d 1300, 1306 (8th Cir. 1991); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984).

[3] Although this Court used the phrase "one-in-a-million" in the case on which the government relies, it was simply noting "*the Appellant*['*s*] suggest[ion] at oral argument that this is that one-in-a-million case where disclosure is necessary." 347 F.3d at 203 (emphasis added).

would, as a practical matter, put the disclosure of FISA materials beyond the reach of *any* criminal defendant. But far from imposing a categorical rule against disclosure, the statute is grounded in Congress's expectation that courts would order disclosure when doing so would substantially promote the accurate determination of a FISA order's legality. *See* S. Rep. No. 701, 95th Cong., 1st Sess. at 64, *reprinted in* 1978 U.S.C.C.A.N. 403.

A. The text of §§ 1806(f) and 1825(g) contemplates disclosure in some cases.

Before FISA, there was no statute authorizing disclosure of foreign surveillance materials to criminal defendants. Consequently, in the four decades of abuses preceding FISA's enactment, private litigants could point to no law or procedural rule requiring disclosure of foreign surveillance materials in the absence of a judicial determination that the Constitution had been violated. If Congress had wanted this pre-FISA practice to prevail for *another* four decades, then it could simply have codified it.[4] But that is not what happened. Instead, three aspects of the disclosure provisions—§§ 1806(f) and

[4] *Cf. Taglianetti v. United States*, 394 U.S. 316, 317–18 (1969) (per curiam) (suggesting that, if a court's task is "'too complex,'" a defendant might be entitled to disclosure of "instances of surveillance which petitioner had standing to challenge under the Fourth Amendment exclusionary rule" (quoting *Alderman v. United States*, 394 U.S. 165, 182 (1968))); *United States v. Falvey*, 540 F. Supp. 1306, 1315 (E.D.N.Y. 1982) ("[T]he massive body of pre-FISA case law of the Supreme Court, this Circuit and others, [held] that the legality of electronic surveillance should be determined on an in camera, ex parte basis.").

1825(g)—require a case-by-case determination rather than an unbroken rule of nondisclosure.

First, the provisions' plain text authorizes disclosure whenever a reviewing court is uncertain about the legality of a contested FISA order. If the court has no doubts about the order's legality—or, indeed, its illegality—then disclosure is not "necessary to make an accurate determination." 50 U.S.C. §§ 1806(f), 1825(g). But if the relevant materials are sufficiently "complex," *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982), or if the court's *ex parte* review cannot rule out the possibility that the court's determination will be mistaken, then disclosure is necessary.

Second, these provisions reject a disclosure scheme that would force courts to automatically defer to the executive branch's judgment about the wisdom of disclosure. Instead, the text of these provisions reflects a congressional expectation that courts would occasionally part ways with the executive branch. Courts are called upon to resolve disclosure issues only *after* the "Attorney General files an affidavit under oath that disclosure . . . would harm the national security of the United States." 50 U.S.C. §§ 1806(f), 1825(g). As it turns out, the Attorney General has filed an affidavit in "every case" in which a defendant has sought suppression or disclosure of FISA materials. David S. Kris & J. Douglas Wilson, 1 *National Security Investigations and Prosecutions*, § 30:7 (2d ed. 2012). But the executive branch's unchanging practice

does not alter—indeed, it underscores—Congress's decision to grant courts the discretion to scrutinize the record and order disclosure in certain cases.

Finally, §§ 1806 and 1825 permit courts to tailor disclosure to the facts of each case. Courts may order disclosure of "portions" of the sought-after materials, and of "summar[ies]" of materials relating to physical searches, "under appropriate security procedures and protective orders." 50 U.S.C. §§ 1806(f), 1825(g). Congress's judgment was therefore that disclosure of FISA materials can be "appropriate," and that carefully controlled disclosure can be preferable to both complete disclosure and complete nondisclosure. Moreover, Congress's subsequent passage of the Classified Information Procedures Act of 1980, 18 U.S.C. App. 3 §§ 1–16, supplies courts with additional means of tailoring disclosures to cleared counsel. *See* Daoud Br. 33–36. Thus, Congress has enacted a disclosure scheme that requires individualized determinations of, rather than a blanket ban on, disclosure.

B. FISA's structure contemplates disclosure in some cases.

FISA's structure confirms that the statutory preference for *in camera* and *ex parte* review is not a bar to court-ordered disclosure. Enacted in the wake of the Watergate scandal and the Church Committee report, FISA was intended to curb surveillance abuses by intelligence agencies. William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 Lewis & Clark L. Rev. 1099, 1110 (2007). So it is hard-

ly surprising that FISA tempers the government's surveillance authority with mechanisms designed to protect individual rights by ensuring that courts can accurately determine the legality of government surveillance.

FISA does this in various ways, which collectively give courts a robust role in ensuring that FISA surveillance is undertaken only when it is based on sufficient legal grounds. For example, FISA generally requires the government to obtain a court order before conducting surveillance or a physical search, and the government cannot obtain such an order without first showing facts justifying a belief that the targeted person "is a foreign power or an agent of a foreign power," and that the targeted facility or place is itself associated with "a foreign power or an agent of a foreign power." 50 U.S.C. §§ 1804, 1823. Likewise, the government must apply for a court order approving the installation of a pen register or trap and trace device, and it must certify that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities," and that an investigation of a United States person is not conducted "solely" based on expression protected by the First Amendment. *Id.* § 1842. And FISA also imposes reporting requirements that enable congressional oversight. *See id.* §§ 1807, 1808, 1826, 1846, 1862, 1871.

Congress also located §§ 1806(f) and 1825(g) within a statutory framework designed to ensure that the legality of FISA orders would be adequately tested in court. FISA requires federal and state agencies to notify an "aggrieved person" whenever a court or other proceeding is likely to involve information "obtained or derived from" FISA surveillance or physical searches. 50 U.S.C. §§ 1806(c), 1806(d), 1825(d), 1825(e). The Supreme Court has stated that these notice provisions ensure meaningful judicial review of foreign surveillance used against "affected persons." *Clapper*, 133 S. Ct. at 1157 (discussing the FISA Amendments Act).

Disclosure is integral to that system of judicial review. FISA's disclosure provisions assure that courts will have the benefit of informed argument from defense counsel when they need it most: that is, when they cannot be sure that *in camera*, *ex parte* review will yield "an accurate determination of the legality of" a FISA order. 50 U.S.C. §§ 1806(f), 1825(g).

C. FISA's legislative history contemplates disclosure in some cases based on a review for complexity.

FISA's legislative history erases any lingering doubt about whether Congress expected courts to actually apply its disclosure provisions. The Senate Judiciary and Intelligence Committees explained that Congress intended to "strik[e] a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself and

mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information." S. Rep. No. 604(I), 95th Cong., 1st Sess. at 57, *reprinted in* 1978 U.S.C.C.A.N. 3959 ("Senate Judiciary Committee Report"); S. Rep. No. 701, 95th Cong., 2d Sess. at 64, *reprinted in* 1978 U.S.C.C.A.N. 4033 ("Senate Intelligence Report").[5] The Committees also described factors that it expected courts to consider when applying the disclosure provisions. Some disclosure would likely be warranted, they noted, when questions about a FISA order's legality were "more complex." *Id.* This might arise from the "volume, scope, and complexity" of the materials, or from other factors, such as "indications of possible misrepresentations of fact." *Id.*

The government's view—that disclosure has never been warranted—does not respect Congress's decision to strike a "reasonable balance." It respects no balance.

In support of its absolutist approach, the government warns that a disclosure order would force it to choose between disclosing sensitive information

[5] *See also* Jimmy Carter, *Foreign Intelligence Surveillance Act of 1978: Statement on Signing S. 1566 into Law* (Oct. 25, 1978) (FISA sought "the correlation between adequate intelligence to guarantee our Nation's security on the one hand, and the preservation of basic human rights on the other"); *Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence of the United States* Senate at 12–13, 95th Cong. (1978) (statement of Hon. Griffin B. Bell) (FISA seeks "a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties").

and forfeiting the use of FISA-derived evidence in court. Gov't Op. Br. 29. That is true, but it is hardly "the very predicament FISA was designed to avert." *Id.* at 33. Congress anticipated precisely that predicament, and it decided that in such cases "the Government must choose—either disclose the material or forgo the use of the surveillance-based evidence." Senate Intelligence Report, *supra*, at 65. Congress knew that, "if the government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed." *Id.*

And Congress well understood that these choices were not merely hypothetical. Congress enacted FISA's disclosure provisions after the Supreme Court ruled, in *United States v. United States District Court for the Eastern District of Michigan (Keith)*, 407 U.S. 297 (1972), that the government was required to disclose unlawfully intercepted conversations to counsel for a defendant accused of plotting to bomb an office of the Central Intelligence Agency. Rather than make that disclosure, the government dropped the charges. *See Sinclair v. Schriber*, 916 F.2d 1109, 1110 (6th Cir. 1990) (describing aftermath of Supreme Court's decision in *Keith*). Thus, the district court's order in this case "impose[s] upon the government" a choice that the government has faced in the past, and which Congress anticipated that the government would face again under FISA. Gov't Op. Br. 29.

II. Revelations about other FISA cases and confusion about the investigation of Daoud demonstrate that the district court did not abuse its discretion by ordering disclosure.

Because the necessity standard turns on the circumstances of this case—and not, as the government implies, on inertia generated by other cases—this appeal requires identifying the various factors that make it difficult to determine the legality of Daoud's surveillance. The government's suggestion that there are no complicating factors here because the district court failed to list them, Gov't Op. Br. 12, 20, wishes away these factors without grappling with them. In ordering disclosure, Judge Coleman acknowledged the necessity standard, cited "a thorough and careful review" of the FISA materials, and cautioned that her order was "not made lightly." SA 5. That ruling is as case-specific as numerous other rulings on FISA's disclosure provisions.[6] Indeed, doubtless because these cases involve sensitive information, the government has readily accepted this analysis when *defending* denials of disclosure.[7] This

[6] *See, e.g.*, *Belfield*, 692 F.2d at 147 (discussing "an examination of the *in camera* Exhibit in this case"); *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (deciding case "after viewing the FISA materials""); *United States v. Sattar*, 2003 WL 22137012, *6 (S.D.N.Y. Sept. 15, 2003) (conducting "a careful independent review of the FISA materials"); *see generally* Kris & Wilson, *supra* § 31:3 (noting that "[m]ost decisions simply state that the court has reviewed the application and order").

[7] *See* Gov't Br., *United States v. Aldawsari*, No. 12-11166, 2013 WL 3913712, at *48–51 (5th Cir. July 18, 2013) (urging affirmance where district court had conducted a "lengthy and considered camera review"); Gov't Br. in Opp. to Pet. for Writ of Cert., *United States v. Squillacote,* No. 00-969, 2001 WL 34117281, at *29 (2001) (arguing "there is no basis for further review of the lower courts' considered determinations on th[e] sensitive and fact-specific question" of necessity for disclosure

case should therefore be decided based on the actual circumstances of the district court's order, rather than misplaced criticisms of its specificity.

Two circumstances stand out: worrisome revelations about inaccuracies that have plagued other FISA cases, and public controversy surrounding the investigation in this case. Those elements were discussed extensively in the proceedings below, and for good reason. R. 51 at 3; R. 52 at 18–21; R. 74 at 3–18; SA 26–27, 36–37. They made Judge Coleman's task in this case far more complex, and disclosure far more necessary.[8]

A. Recently disclosed information about FISA litigation has amplified the complexity of this case.

Judge Coleman was required to resolve this case's disclosure issue during a unique historical moment. Over the past nine months, an enormous amount of information about the government's surveillance activities has been made public. These disclosures have revealed crucial government miscommunications about both its surveillance practices and its interpretations of FISA

---

where the "district found, 'after review,' that there was 'no basis for discovery or an adversary hearing.'"); Gov't Br., *United States v. Hasan*, No. 12-50841, 2013 WL 266759, at *19 (5th Cir. Jan. 16, 2013) (arguing that the district court had "conducted 'a thorough in camera, ex parte review' of the FISA materials at issue").

[8] The court's word choices—writing "may be" instead of "is," and discussing what is "best"—are meager grounds for reversal. *See* Gov. Op. Br. 20–28. Appellate courts usually do not require district courts to "recite 'magic words.'" *United States v. Chavers*, 515 F.3d 722, 725–26 (7th Cir. 2008) ("so long as the district court substantively complie[s] with the requirements for evaluating a motion to withdraw a guilty plea, the court need not recite formulaic language").

terminology. These developments injected uncertainty into FISA litigation just as this case was unfolding. And if the government's miscommunications are attributable to good-faith errors that could inadvertently recur—as opposed to intentional misconduct that has been stamped out—then they are even *more* acutely relevant here. Thus, these new developments created the kind of complexity that can make disclosure necessary. *See* Senate Judiciary Report, *supra*, at 57; Senate Intelligence Report, *supra*, at 64.

1. Miscommunications about facts.

Recently declassified FISC opinions state that the government's surveillance applications have included "substantial misrepresentation[s] regarding the scope of a major collection program." *[Redacted],* 2011 WL 10945618, at *5 n.14 (FISC Oct. 3, 2011) (Bates, J.); *see* R. 74 at 4–10. For instance, inaccurate government submissions tainted the FISC's analysis of "upstream collection" of telephone and internet communications under Section 702 of the FAA. *[Redacted],* 2011 WL 10945618, at *5 n.14.[9] The FISC's approval of this program depended on the government's representations about its scope, including the notion that the program would collect communications only be-

[9] The redacted FISC opinion states that "the term 'upstream collection' refers to NSA's interception of Internet communications as they transit [redacted] rather than acquisitions directly from internet services providers such as [redacted]." 2011 WL 10945618, at *2 n.3. This program appears to collect data from the "internet backbone"—the principal data routes between the interconnected networks and core routers on the internet—rather than from the internet companies.

tween or among individual account users who had been targeted, and "about" communications containing a reference to a targeted account. *Id.* at *5–6, *9–11, *25–26.

Yet years after the program began, the government revealed that it collected "multiple discrete communications," that likely included tens of thousands communications that were neither to, from, nor about targeted accounts. *Id.* at *5, *11–12, *15, *33–37. "That revelation fundamentally alter[ed] the Court's understanding of the scope of the collection conducted pursuant to [the program] and require[d] careful reexamination of many of the assessments and presumptions underlying its prior approvals." *Id.* at *5. Because "two fundamental underpinnings of the Court's prior assessments no longer held true," *id.* at *10, the FISC concluded that aspects of the "upstream collection" were "deficient on statutory and constitutional grounds," *id.* at *1.

Similarly, when the FISC authorized the government's bulk collection of "call detail records" in 2006, it relied on the government's claim that it would strictly control access to the resulting trove of data about phone calls by innocent Americans. *In re Production of Tangible Things From [Redacted],* No. BR 08-13, 2009 WL 9150913, at *1, *5 (FISC Mar. 2, 2009) (Walton, J.). The government repeatedly insisted that it would access the trove only to search for information pertaining to phone numbers that satisfied a "reasonable, ar-

ticulable suspicion," or "RAS," standard. *Id.* at *1–4. But that is not what happened.

In 2009, the government informed the FISC that it consistently ran an "alert list" of phone numbers—the vast majority of which were not supported by reasonable, articulable suspicion—against the bulk data collection. *Id.* at *2 & n.2. Thus, it "c[a]me to light that the FISC's authorizations of this vast collection program [were] premised on a flawed depiction of how the NSA uses [telephony] metadata. *Id.* at *5. This critical misperception was "buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." *Id.* Armed with accurate information, the FISC reevaluated the legality of the program and narrowed the government's querying abilities. *Id.* at *5–6, *9.

2. Miscommunications about legal terms.

This case is also complicated by revelations of the government's failure to clearly inform courts of its interpretations of vitally important FISA terms. R.74 at 11–12. These miscommunications have disconnected the activities that courts believe the government is undertaking from the activities that the government is actually undertaking. And their effect on FISA litigation is insidious; they can damage a court's decision-making process precisely because

they can arise even when the lawyers appearing before the court are acting in good faith.

For example, when the government told the FISC that it had been impermissibly checking bulk telephone data against phone numbers not supported by reasonable, articulable suspicion, it did not simply confess error. It sought to attribute that error, at least in part, to "a belief by some personnel within the NSA that some of the [FISC's] restrictions on access to the [Business Record] metadata applied only to 'archived data,' *i.e.*, data residing within certain databases at the NSA." *In re Production of Tangible Things From [Redacted],* 2009 WL 9150913, at *2. But "[t]hat interpretation of the Court's Orders," wrote FISC Judge Reggie B. Walton in May 2009, "strain[ed] credulity." *Id.*

It is unclear when the relevant "personnel within the NSA" shared their strained interpretation with the government's lawyers at the FISC. But, no matter the timing, Judge Walton's opinion raised doubts about whether courts can reliably predict how the government has interpreted, or will interpret, its FISA obligations.

A similar problem has affected proceedings at the U.S. Supreme Court and at a federal district court in Oregon. At the Supreme Court, the government successfully argued in *Clapper v. Amnesty International* that various lawyers, scholars, and journalists lacked standing to challenge surveillance under the

FAA. The Solicitor General told the Court that the FAA would more appropriately be challenged by someone who "gets notice that the government intends to introduce information in a proceeding against them." Oral Argument Tr. at 4, *Clapper*, 133 S. Ct. 1138. But, in fact, no one received notice. At the time of *Clapper*, the government's practice was to *not* notify criminal defendants if information had been collected about them under the FAA. That practice was reportedly based on intelligence officials' peculiar view about when evidence has been "derived from" the FAA for purposes of § 1806(c). *See* Charlie Savage, *Door May Open to Challenge Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, at A3 (Oct. 16, 2013); R.74-2 (letter from Senators Udall, Wyden & Heinrich to Solicitor General Verrilli).

The Solicitor General appeared to be unaware of the government's true practice when *Clapper* was argued. And although the government has since changed its practice, the opinion in *Clapper* may have rested on the Solicitor General's misapprehension. 133 S. Ct. at 1154 (stating that, in light of FISA's notice requirement, "our holding today by no means insulates [the FAA] from judicial review").

What is more, the government's understanding of the term "derived from" appears to have had real consequences in a criminal case, much like this one, before Judge Garr M. King of the District of Oregon. There, a jury convicted a defendant in January 2013 of a crime involving a plot to detonate a car bomb.

Although the case was indicted in November 2010, and although the defendant's pretrial motions requested disclosure of FAA materials, the defendant was not notified until August 2013—after the 14-day trial and after the verdict—that the government's case against him involved FISA materials that were themselves derived from prior FAA collection. *See* Opinion and Order at 2, *United States v. Mohamud*, No. 3:10-cr-475 (D. Or. Mar. 19, 2014).

Those episodes could inform, in at least two respects, a federal court's ruling on whether disclosure of FISA materials is "necessary to make an accurate determination of the legality" of a particular FISA order. First, a court could reasonably worry that the government's written and oral submissions rest on a self-serving understanding of its FISA obligations. Second, a court could reasonably worry that, just like the Solicitor General in *Clapper*, the government's lawyers in a FISA case might not fully grasp the government's own practices. SA 17, 35; *see also* Daoud Br. 33 n.34. Under the statute, an adversarial process informed by tailored disclosure to defense counsel is the appropriate answer to this uncertainty.

B. Uncertainty about the government's surveillance in this case has heightened its complexity.

The lesson of these recent disclosures—that judicial decision-making has at times been hampered by unchallenged reliance on the government—applies with particular force to this case. First, this case has been the subject

of uncertainty and controversy about whether the government's investigation of Daoud involved the FISA Amendments Act. Because the FAA's constitutionality has not been adjudicated, disclosure of FISA materials would be necessary in this case if there any possibility that the government used the FAA in its investigation of Daoud. Second, even if there is no such possibility, against the backdrop of recent disclosures, the general confusion surrounding this case is the kind of complexity that warrants disclosure.

Questions about the surveillance used in this case began on December 27, 2012, when Senator Dianne Feinstein referred to Daoud's arrest on the Senate floor. Speaking in favor of reauthorizing the FAA, Senator Feinstein described several people arrested for terrorist plots in 2012, including Adel Daoud. R. 42-2. She concluded that "the FISA Amendments Act is important and these cases show the program has worked." *Id.* That statement ignited a controversy about this case because Daoud had not received notice that the government intended to use against him evidence derived from FAA surveillance. In response, counsel for the Senate Intelligence Committee has insisted that Senator Feinstein did not mean to imply that the FAA had actually been used against Daoud, R.70-2, and the government has claimed that it "does not intend to use any such evidence obtained or derived from FAA-authorized surveillance in the course of this prosecution." R.49 at 2. Even so, Senator Feinstein's remarks remain relevant.

For starters, given the government's track record when interpreting FISA's notice provisions, its claim that FAA notice is not required in this case does not rule out the possibility that the FAA played some role in the investigation of Daoud. It remains unclear, after all, how the government decides when evidence is "derived from" FAA surveillance, and thus when it believes notice is required. And if there is any chance that FAA surveillance played a role in this case, then disclosure of the relevant materials would be necessary for the district court to make an accurate determination of the legality of any FISA order that was itself the fruit of FAA surveillance. The FAA's constitutionality has never been adjudicated, and there is good reason to doubt that the FAA could survive such adjudication.

The FAA substantially revised the FISA regime and authorized the acquisition of a wide swath of communications from internet and telecommunications providers inside the United States. Unlike FISA, the FAA authorizes surveillance that is not predicated on individualized suspicion or probable cause. *See* 50 U.S.C. § 1881a(a) & (g); Kris & Wilson, *supra*, § 16:16. Instead, the FISC reviews and approves only the targeting and minimization procedures the government proposes to use in carrying out its surveillance. 50 U.S.C. § 1881a(g). Although the government cannot "intentionally target any person known at the time of the acquisition to be located in the United States," 50 U.S.C. § 1881(a)(B), it appears the government uses the FAA to

sweep up the international communications of U.S. citizens and residents whom it does not regard as intentional targets. *Cf. FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary,* 109th Cong. 9 (2006), http:/1.usa.gov/1kbgHm3 (statement of NSA Director Michael Hayden) (stating, with respect to the FAA's predecessor statute, that certain communications "with one end . . . in the United States" are "the most important to us"). In this way, the FAA exposes every communication between an individual in the United States and a non-American abroad to potential surveillance.

Those procedures raise serious questions under the Fourth Amendment. *See* Def. Mot. to Suppress at 20–44, *United States v. Muhtorov*, No. 12-cr-0003-JLK-1 (D. Colo. Jan. 29, 2014). And if the government improperly failed to notify Daoud under the FAA, that failure would itself raise difficult constitutional issues. *See, e.g.*, Def. Memo. in Support of Mot. to Suppress at 1–3, *United States v. Mohamud*, No. 3:10-cr-475 (D. Or. Apr. 4, 2014) (arguing that the government's belated FAA notice could implicate *Brady* and due process).

Alternatively, the complete absence of any FAA role in this case might have been cold comfort to Judge Coleman. Under that scenario, Senator Feinstein's willingness to cite this case as justification for renewing the FAA—or someone else's willingness to advise Senator Feinstein to do so—would be yet another example of a government official creating confusion about the true

facts of a FISA case. This makes disclosure more necessary, rather than less, because it presents the possibility of a mistake about the facts of this very case. *Cf.* Senate Judiciary Report, *supra*, at 57 (referring to "indications of possible misrepresentations"); Senate Intelligence Report, *supra*, at 64 (same). Thus, even if Judge Coleman was convinced that the FAA was not used against Daoud, she might reasonably have wondered whether the FAA controversy was evidence that some other aspect of this case could benefit from careful review by defense counsel. Rather than risk learning of a mistake after the fact—as Judge Walton did at the FISC and Judge King did in the District of Oregon—Judge Coleman appropriately ordered disclosure now.

* * *

Given the circumstances that confronted the district court, affirming its disclosure order would support rather than undermine the congressional judgment at the core of FISA: that it is possible to protect both national security and civil liberties. Just as important, affirming the district court would avoid serious constitutional questions. Although courts have rejected constitutional challenges to the *in camera*, *ex parte* procedures of §§ 1806 and 1825, *no court* has done so following another court's finding that disclosure of FISA

materials "may be necessary" to determine a FISA order's legality.[10] Unless this Court is prepared to say that the district court's finding was clearly erroneous—which, on this record, it plainly was not—then it is unclear how the Constitution could tolerate sidelining counsel whose involvement may be necessary to get the case right. *See Evitts v. Lucey*, 469 U.S. 387, 395 (1985) ("[T]he Constitution cannot tolerate trials in which counsel, though present in name, is unable to assist the defendant to obtain a fair decision on the merits").

CONCLUSION

Amici respectfully request that this Court affirm the order below.

[10] *Cf. United States v. El-Mezain*, 664 F.3d 467, 566–68 (5th Cir. 2011) (no due process violation where the district court did "not believe that disclosing the applications and related materials to defense counsel would assist the court"); *United States v. Stewart*, 590 F.3d 93, 126–129 (2d Cir. 2009) (no due process violation where the district court reviewed the materials and "concluded that this was not a case where disclosure of the classified FISA materials was necessary").

Respectfully submitted.

/s/ Matthew R. Segal

Patrick Toomey
Brett Max Kaufman
Jameel Jaffer
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Tel: 212-549-2500
Fax: 212-549-2654

Matthew R. Segal
Jessie J. Rossman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MASSACHUSETTS
211 Congress Street, 3d Floor
Boston, MA 02110
Tel: 617-482-3170
Fax: 617-451-0009

Harvey Grossman
THE ROGER BALDWIN FOUNDATION OF ACLU, INC.
180 North Michigan Avenue
Suite 2300
Chicago, Illinois 60601
Tel: 312-201-9740
Fax: 312-201-9760

Hanni Fakhoury
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: 415-436-9333
Fax: 415-436-9993

Dated: May 9, 2014

CERTIFICATE OF COMPLIANCE WITH FED. R. APP. P. 32(a)

1. This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) and Fed. R. App. P. 29(d) because:

   This brief contains 6,221 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), as calculated by the word-counting function of Microsoft Office 2010.

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally-spaced typeface using Microsoft Word in 13-point Century Schoolbook, with 12-point Century Schoolbook footnotes.

DATED: May 9, 2014

/s/ Matthew R. Segal
Matthew R. Segal
Counsel for *Amici Curiae*

CERTIFICATE OF SERVICE

I hereby certify that on May 9, 2014, I electronically filed the foregoing BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF ILLINOIS, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DE-FENDANT-APPELLEE AND URGING AFFIRMANCE with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Respectfully submitted.

/s/ Matthew R. Segal
Matthew R. Segal
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MASSACHUSETTS
Congress Street, 3d Floor
Boston, MA 02110
Tel: 617-482-3170
Fax: 617-451-0009

Counsel for *Amici*