

NO. 18-1366

**IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT**

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

JAMSHID MUHTOROV,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
District of Colorado (Denver)
District 1082-1, Case No. 1:12-CR-00033-JLK-1

The Honorable John L. Kane, Junior, Senior United States District Judge

**BRIEF OF AMICI CURIAE CHURCH COMMITTEE STAFF
IN SUPPORT OF DEFENDANT-APPELLANT
JAMSHID MUHTOROV AND REVERSAL**

Andrew Crocker
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
andrew@eff.org
amackey@eff.org
(415) 436-9333

Counsel for Amici Curiae

TABLE OF CONTENTS

STATEMENT OF INTEREST 1

INTRODUCTION 1

ARGUMENT 2

 I. CONGRESS INTENDED FISA TO MANDATE DISCLOSURE OF SURVEILLANCE MATERIALS TO DEFENSE COUNSEL, UNDER APPROPRIATE SECURITY PROCEDURES, IN AT LEAST SOME CASES. 2

 A. The text of §§ 1806(f) and 1825(g) contemplates disclosure in some cases rather than automatic deference to the executive branch. 5

 B. FISA’s structure contemplates disclosure in some cases..... 7

 C. FISA’s legislative history contemplates disclosure in some cases based on a review for complexity..... 9

 II. ADDITIONAL CONSIDERATIONS BEAR ON DISCLOSURE UNDER FISA, SUCH AS THE NOVELTY OR COMPLEXITY OF SURVEILLANCE, AS IN THIS CASE INVOLVING SECTION 702 SURVEILLANCE. 11

CONCLUSION 17

CERTIFICATE OF COMPLIANCE 18

CERTIFICATE OF DIGITAL SUBMISSION 19

CERTIFICATE OF SERVICE 20

TABLE OF AUTHORITIES

Cases

<i>[Redacted]</i> , (FISC Apr. 26, 2017).....	15, 16
<i>[Redacted]</i> , 2011 WL 10945618 (FISC Oct. 3, 2011).....	14, 15, 16
<i>[Redacted]</i> , 2011 WL 10947772 (FISC Nov. 30, 2011).....	16
<i>Alderman v. United States</i> , 394 U.S. 165 (1968)	5
<i>Clapper v. Amnesty Int’l, USA</i> , 133 S. Ct. 1138 (2013)	9, 14
<i>Fazaga v. FBI</i> , 916 F.3d 1202 (9th Cir. 2019)	3
<i>In re Kevork</i> , 788 F.2d 566, 569 (9th Cir. 1986)	2
<i>In re Proceedings Required by § 702(i) of FISA Amendments Act</i> , 2008 WL 9487946 (FISC Aug. 27, 2008).....	13
<i>Sinclair v. Schriber</i> , 916 F.2d 1109 (6th Cir. 1990)	11
<i>Taglianetti v. United States</i> , 394 U.S. 316 (1969)	5
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982).....	6, 12
<i>United States v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974)	12
<i>United States v. Daoud</i> , 755 F.3d 749 (7th Cir. 2014)	5

United States v. Falvey,
540 F. Supp. 1306 (E.D.N.Y. 1982) 5

United States v. Muhtorov,
187 F. Supp. 3d. 1240 (D. Colo. 2015)..... 2

*United States v. United States District Court for the Eastern District of Michigan
(Keith)*,
407 U.S. 297 (1972) 11

Statutes

18 U.S.C. App. 3 §§ 1–16 7

50 U.S.C. § 1804 8

50 U.S.C. § 1805 12

50 U.S.C. § 1806 *passim*

50 U.S.C. § 1807 8

50 U.S.C. § 1808 8

50 U.S.C. § 1823 8

50 U.S.C. § 1824 12

50 U.S.C. § 1825 *passim*

50 U.S.C. § 1826 8

50 U.S.C. § 1842 8

50 U.S.C. § 1846 8

50 U.S.C. § 1862 8

50 U.S.C. § 1871 8

50 U.S.C. § 1881a 13

Legislative Materials

Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence of the United States Senate, 95th Cong. (1978).. 10

S. Rep. No. 94-755 (1976)..... 3

S. Rep. No. 95-604(I) (1978),
reprinted in 1978 U.S.C.C.A.N. 3904 3, 4, 10

S. Rep. No. 95-701,
reprinted in 1978 U.S.C.C.A.N. 3973 *passim*

Other Authorities

David S. Kris & J. Douglas Wilson, 1 *National Security Investigations and Prosecutions* (2d ed. 2012)..... 6

Jimmy Carter, *Foreign Intelligence Surveillance Act of 1978: Statement on Signing S. 1566 into Law* (Oct. 25, 1978)..... 10

Office of the Director of National Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities Calendar Year 2018* (Apr. 2019)..... 13, 14

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) 14, 15

William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 *Lewis & Clark L. Rev.* 1099 (2007) 7

STATEMENT OF INTEREST¹

Amicus Peter Fenn served as Washington Chief of Staff for Senator Frank Church during his committee's intelligence investigation and on the staff of the Senate Intelligence Committee.

Amicus Loch Johnson served as special assistant to the chair of the Church Committee and as staff director of the House Subcommittee on Intelligence Oversight. He also worked with the Chair of the Aspin-Brown Commission on Intelligence. He is currently Regents Professor of International Affairs Emeritus at the University of Georgia and recently retired as the editor of Intelligence and National Security. From his firsthand experiences with the Church Committee investigations and the Aspin-Brown Commission, Mr. Johnson is directly familiar with the complex features of American intelligence agencies and their oversight.

INTRODUCTION

Amici, former staff of the Church Committee, write to discuss the standard for disclosure of information obtained or derived from the acquisition of foreign intelligence information under the Foreign Intelligence Surveillance Act of 1978

¹ The parties have consented to the filing of this brief. No person other than amici or their counsel has made any monetary contributions intended to fund the preparation or submission of this brief. No party's counsel prepared this brief in whole or in part. Counsel for amici and members of Defendant-Appellant's counsel previously filed a brief raising similar arguments in *United States v. Daoud*, 755 F.3d 749 (7th Cir. 2014).

(“FISA”) and Section 702 of the FISA Amendments Act of 2008 (“Section 702”). When the district court denied Mr. Muhtorov’s motion for discovery of information derived from Section 702 surveillance in this case,² it disregarded FISA’s clear direction—and the stated intent of Congress—that disclosure may be appropriate in specific cases, particularly cases like Mr. Muhtorov’s that involve complex or novel surveillance.

ARGUMENT

I. CONGRESS INTENDED FISA TO MANDATE DISCLOSURE OF SURVEILLANCE MATERIALS TO DEFENSE COUNSEL, UNDER APPROPRIATE SECURITY PROCEDURES, IN AT LEAST SOME CASES.

FISA reflects Congress’s judgment that identifying and monitoring foreign threats can be accomplished without compromising civil liberties. *See, e.g., In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986). FISA’s enactment followed the

² In this case, the government notified appellant Jamshid Muhtorov that it intended to offer, or otherwise use or disclose, evidence obtained or derived from FISA surveillance, 50 U.S.C. §§ 1801–1811, 1821–1829. District Ct. Dkt. 12. Over a year and half later, the government again notified Mr. Muhtorov of its intent to use further FISA evidence obtained through warrantless surveillance under Section 702. District Ct. Dkt. 457. In response to Mr. Muhtorov’s renewed Motion to Suppress and Motion for Discovery, the government filed an affidavit from Attorney General Eric Holder stating that disclosure of any of the FISA materials would harm national security. District Ct. Dkt. 559-1. In denying Mr. Muhtorov’s motion, the district court reviewed these materials *ex parte* and *in camera*, but did not explicitly address his argument that disclosure to defense counsel was “necessary” to determine the legality of the surveillance. *United States v. Muhtorov*, 187 F. Supp. 3d. 1240, 1258 (D. Colo. 2015).

investigation into wrongdoing by intelligence agencies by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the Church Committee. *Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II)*, S. Rep. No. 94-755, at 1 (1976). The agencies had “violated specific statutory prohibitions,” “infringed . . . constitutional rights,” and “intentionally disregarded” statutory restrictions. *Id.* at 137; *Fazaga v. FBI*, 916 F.3d 1202, 1233 (9th Cir. 2019) (describing Church Committee’s findings). In response, Congress passed FISA to regulate the government’s ability to conduct electronic surveillance and physical searches undertaken to protect national security. The statute details roles for all three branches of government, providing judicial and congressional oversight of the covert surveillance activities by the executive branch, combined with measures to safeguard secrecy necessary to protect national security.

Relevant to this case, Congress recognized that “delicate problems and competing interests” are raised when defendants seek access to materials derived from surveillance. S. Rep. No. 95-604(I) at 53 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3954 (“Senate Judiciary Committee Report”); S. Rep. No. 95-701 at 59, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4028 (“Senate Intelligence Committee Report”). “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.” *Id.* Therefore, the statute authorizes courts to order disclosure of classified materials, when “necessary,” to the targets of FISA surveillance. 50 U.S.C. §§ 1806(f), 1825(g).

The government must notify “aggrieved persons” who were subject to electronic or physical surveillance 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. *Id.* §§ 1806(f), 1825(g). After that review, the court may order disclosure to the aggrieved 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).

However, the executive branch has taken the position that disclosure to a defendant’s counsel would harm national security in every single case where disclosure has been sought, including this one. And, to date, only one district court has determined that, notwithstanding the Attorney General’s submission, disclosure is “necessary,” only to be overturned on appeal. *See United States v. Daoud*, 755

F.3d 749 (7th Cir. 2014). The lack of disclosure in even a single case is inconsistent with the clear intent of Congress in FISA, which plainly contemplates that disclosure will occur in some cases, despite the wishes of the executive branch.

A. The text of §§ 1806(f) and 1825(g) contemplates disclosure in some cases rather than automatic deference to the executive branch.

Before FISA, there was no statute authorizing disclosure of foreign surveillance materials to criminal defendants. Consequently, in the four decades of abuses cataloged by the Church Committee 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 to replicate this practice as part of FISA, it could simply have codified it.³ But that is not what happened. For at least three reasons, the disclosure provisions—§§ 1806(f) and 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

³ 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.”).

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 “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. 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.

Because FISA gives courts authority to oversee the executive branch’s foreign intelligence surveillance activities at multiple stages, the law’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 hardly 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 (a)(3), 1823(a)(3). 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(c)(2). 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 electronic 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 person[s].” *Clapper v. Amnesty Int’l, USA*, 133 S. Ct. 1138, 1154 (2013) (discussing the FISA Amendments Act).

And, as discussed above, Congress permitted courts to review those materials *ex parte* and *in camera*, to order the disclosure of those materials in some cases, and to tailor those disclosures to address concerns about disclosing information that would harm national security.

Disclosure under FISA is thus integral to that system of judicial review Congress created in enacting the law. 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.” Senate Judiciary Committee Report, S. Rep. No. 95-604(I), at 57, 1978 U.S.C.C.A.N. 3959; Senate Intelligence Committee Report, S. Rep. No. 95-701, at 64, 1978 U.S.C.C.A.N. 4033.⁴ The reports emphasized that “[t]he decision whether it is necessary to order disclosure to a person is *for the Court to make*,” not the executive branch. *Id.* (emphasis added).

And when a court determines that disclosure of FISA-derived evidence to the defense is warranted, Congress anticipated precisely that the government might be forced to decide between actually disclosing this evidence or forfeiting its use in court. In such cases, Congress declared that “the Government must choose—either disclose the material or forgo the use of the surveillance-based evidence.” Senate Intelligence Committee Report, S. Rep. No. 95-701, at 65, 1978 U.S.C.C.A.N. 4034.

⁴ 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”).

“[I]f the government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed.” *Id.*

These considerations were not merely hypothetical at the time of the statute’s passage. 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, 1111 (6th Cir. 1990) (describing aftermath of Supreme Court’s decision in *Keith*).

The government’s view—that disclosure has never been warranted in the history of FISA—does not respect Congress’s decision to strike a “reasonable balance.” It respects no balance.

II. ADDITIONAL CONSIDERATIONS BEAR ON DISCLOSURE UNDER FISA, SUCH AS THE NOVELTY OR COMPLEXITY OF SURVEILLANCE, AS IN THIS CASE INVOLVING SECTION 702 SURVEILLANCE.

Congress also recognized that disclosure would likely be warranted under FISA in cases raising novel or complex surveillance concerns. In their authoritative reports on FISA, the Senate Intelligence and Judiciary Committees further described factors that Congress expected courts to consider when applying the statute’s

disclosure provisions. Some disclosure would likely be warranted, they noted, when questions about a FISA order's legality were "more complex." Senate Intelligence Committee Report, S. Rep. 95-701, at 64, 978 U.S.C.C.A.N. at 4033. This might arise from the "volume, scope, and complexity" of the materials, or from other factors, such as "indications of possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order." *Id.* (citing *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir. 1974) (en banc) (describing disclosure as justified by an "exercise of . . . discretion" where "adversary presentation would substantially promote a more accurate decision)).

While FISA's necessity standard anticipates that disclosure will be an exception rather than a categorical rule in every case, a confluence of the factors mentioned in the Senate reports can clearly create such complexity that disclosure is necessary. *Belfield*, 692 F.2d at 147.

Cases that involve surveillance under Section 702, such as this one, are necessarily more complex than those that only involve surveillance conducted pursuant to "traditional" FISA orders. While traditional FISA orders require "probable cause to believe that the target . . . is a foreign power or an agent of a foreign power," 50 U.S.C. §§ 1805(a)(2), 1824(a)(2), Section 702 authorizes the

executive branch to conduct programmatic surveillance that is not based on probable cause or individualized suspicion. *See* 50 U.S.C. § 1881a.

Closely related, the role of the Foreign Intelligence Surveillance Court (“FISC”) is much more “narrowly circumscribed” under Section 702 than in traditional FISA proceedings. *In re Proceedings Required by § 702(i) of FISA Amendments Act*, Misc. No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008). Under Section 702, the government need not make a demonstration of probable cause to surveil specific targets, nor is required to even inform the court of its specific targets, or the communications facilities where its surveillance will occur. *See* 50 U.S.C. § 1881a. The FISC’s role is limited to reviewing annual submissions by the executive branch that describe its surveillance programs in broad, programmatic terms, including the targeting, minimization, and querying procedures the government will follow. *Id.* § 1881a(j). In response, the FISC reviews these “procedures and guidelines” to ensure they comply at a programmatic level with the Fourth Amendment and the statute’s requirements. *Id.* § 1881a(h).

Surveillance under Section 702 is both vast in scope and novel in type. The Office of the Director of National Intelligence (ODNI) reported that, in 2018 it monitored the communications of 164,770 targets under a single FISC order.⁵ In

⁵ Office of the Director of National Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities Calendar Year 2018* at 13 (Apr. 2019) (“2018 ODNI Transparency Report”),

2011, when it monitored a smaller number of targets, the government nevertheless collected more than 250 million communications. *[Redacted]*, 2011 WL 10945618, at *9 (FISC Oct. 3, 2011). Today, with more than double as many targets as five years ago, the government likely collects over a billion communications under Section 702 each year.⁶ As the Privacy and Civil Liberties Oversight Board observed, “the expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications.”⁷ Moreover, the passage of the FISA Authorization Act and Section 702 in particular were designed to allow the intelligence community to keep up with cutting-edge communication technology, which the executive branch argued could not be adequately addressed by FISA’s original statutory framework. *See Clapper v. Amnesty Int’l, USA*, 133 S. Ct. at 1144. Section 702 is therefore

https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

⁶ Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* at 116 (July 2, 2014) (“PCLOB Report”), <https://www.pclob.gov/library/702-Report.pdf> (noting that the “current number [in 2014 wa]s significantly higher” than in 2011). According to ODNI, the number of targets of Section 702 surveillance nearly doubled between 2014 and 2018. 2018 ODNI Transparency Report at 13.

⁷ PCLOB Report at 116.

especially likely to raise novel technical challenges, even for members of the executive branch conducting surveillance authorized under the statute.⁸

The FISC’s limited role in assessing the executive branch’s programmatic plans for Section 702 surveillance and the scope and complexity of this surveillance have at times led the court to issue rulings based on false premises. For example, in 2011 the court learned of “substantial misrepresentation[s] regarding the scope of a major collection program,” the so-called Upstream collection of telephone and internet communications under Section 702. *[Redacted]*, 2011 WL 10945618, at *5 n.14 (FISC Oct. 3, 2011). The FISC explained that its approval of this program depended on the government’s representations about its scope, including the notion that the program would collect communications only between 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 in 2011, 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

⁸ *See, e.g.*, PCLOB Report at 40 (discussing NSA’s acquisition of so-called multi-communication transactions (“MCTs”) and its difficulty in processing them pursuant to applicable minimization procedures); *[Redacted]*, No. *[Redacted]*, at 19 (FISC Apr. 26, 2017) (continuing technical challenges in processing MCTs) (“April 26, 2017 FISC Op.”), available at https://www.aclu.org/sites/default/files/field_document/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

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 h[e]ld true,” *id.* at *10, the FISC concluded that aspects of the “upstream collection” were “deficient on statutory and constitutional grounds,” *id.* at *1. The court’s subsequent approval of Upstream was based only on the government’s modification of its procedures to prohibit the use of US-person identifiers to query Upstream collection. *See [Redacted]*, 2011 WL 10947772, at *1 (FISC Nov. 30, 2011).

Nevertheless, in 2017, the FISC again learned of “significant noncompliance” with these modified procedures, “suggesting that the problem was widespread during all periods under review,” perhaps dating back to 2011. April 26, 2017 FISC Op. at 4, 19. The court attributed this “institutional lack of candor” by the government, which prohibited it from adequately assessing the legality of the government’s conduct. *Id.* at 19-20.

In light of these factors—the volume, scope and complexity of Section 702 surveillance as well as a years-long pattern of misrepresentations by the executive branch to the court overseeing this surveillance—disclosure of the FISA-materials under appropriate security procedures may be appropriate in this case.

CONCLUSION

For the reasons stated above, Amici respectfully ask the Court to apply to the appropriate standard for disclosure under FISA.

Respectfully submitted,

/s/ Andrew Crocker

Andrew Crocker

Aaron Mackey

Electronic Frontier Foundation

815 Eddy Street

San Francisco, California 94109

andrew@eff.org

amackey@eff.org

(415) 436-9333

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amicus Curiae* Electronic Frontier Foundation in Support of Defendant-Appellant Jamshid Muhtorov and Reversal complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 3,840 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

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 2016, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: October 7, 2019

By: /s/ Andrew Crocker
Andrew Crocker

Counsel for Amici Curiae

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

- (1) all required privacy redactions have been made per 10th Cir. R. 25.5;
- (2) if required to file additional hard copies, that the ECF submission is an exact copy of those documents;
- (3) the digital submissions have been scanned for viruses with the most recent version of a commercial virus-scanning program, Avast Mac Security Version 14.2, updated October 3, 2019, and according to the program are free of viruses.

Dated: October 7, 2019

By: /s/ Andrew Crocker
Andrew Crocker

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I certify that on this 7th day of October, 2019, I electronically filed the foregoing Brief of Amicus Curiae using the Court's CM/ECF system which will send notification of such filing to the following:

James Murphy, james.murphy3@usdoj.gov

Joseph Palmer, joseph.palmer@usdoj.gov

John C. Arceci, john_arceci@fd.org

Ashley Gorski, agorski@aclu.org

Patrick Toomey, ptoomey@aclu.org

Dated: October 7, 2019

By: /s/ Andrew Crocker
Andrew Crocker

Counsel for Amici Curiae