

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
For the District of Colorado, No. 1:12-cr-00033-JLK
Honorable John L. Kane

**BRIEF FOR AMICUS CURIAE NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS IN SUPPORT OF APPELLANT AND
URGING REVERSAL**

Norman R. Mueller
HADDON, MORGAN AND
FOREMAN, P.C.
150 East 10th Avenue
Denver, CO 80203
Telephone: (303) 831-7364
National Association of Criminal
Defense Lawyers, Amicus
Committee Co-Chair

John D. Cline
LAW OFFICE OF JOHN D. CLINE
One Embarcadero Center, Suite 500
San Francisco, CA 94111
Telephone: (415) 662-2260

Attorneys for Amicus Curiae
NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS

CORPORATE DISCLOSURE STATEMENT

Amicus curiae National Association of Criminal Defense Lawyers submits the following corporate disclosure statement, as required by Fed. R. App. P. 26.1 and 29(c): NACDL is a nonprofit corporation organized under the laws of the District of Columbia. It has no parent corporation, and no publicly held corporation owns ten percent or more of its stock.

DATED: October 7, 2019

Respectfully submitted,

/s/ John D. Cline
John D. Cline

Attorney for Amicus Curiae
National Association of Criminal
Defense Lawyers

TABLE OF CONTENTS

	Page
INTEREST OF AMICUS CURIAE.....	1
SUMMARY OF THE ARGUMENT	2
ARGUMENT	4
I. MUHTOROV'S "PRIVATE INTEREST"	5
II. THE RISK OF ERRONEOUS DEPRIVATION AND THE VALUE OF ADDITIONAL PROCEDURES	6
III. THE GOVERNMENT'S INTEREST	13
CONCLUSION	20

TABLE OF AUTHORITIES

	Page
CASES	
<i>Ake v. Oklahoma</i> , 470 U.S. 68 (1985)	5
<i>Alderman v. United States</i> , 394 U.S. 165 (1969)	7, 8
<i>American-Arab Anti-Discrimination Committee v. Reno</i> , 70 F.3d 1045 (9th Cir. 1995).....	4, 6, 7
<i>Brady v. Maryland</i> , 373 U.S. 83 (1963)	4
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978)	2, 8, 9, 10
<i>In re All Matters</i> , 218 F. Supp. 2d 611 (FISC), <i>rev'd</i> , 310 F.3d 717 (FISCR 2002)	11
<i>In re FBI</i> , 2009 U.S. Dist. LEXIS 132935 (FISC Sept. 25, 2009).....	12
<i>In re Washington Post Co.</i> , 807 F.2d 383 (4th Cir. 1986).....	19
<i>Jencks v. United States</i> , 353 U.S. 657 (1957)	20
<i>Johnson v. United States</i> , 333 U.S. 10 (1948)	12
<i>Kiareldeen v. Reno</i> , 71 F. Supp. 2d 402 (D.N.J. 1999)	5, 7
<i>Kindhearts for Charitable Humanitarian Development, Inc. v. Geithner</i> , 710 F. Supp. 2d 637 (N.D. Ohio 2010)	4
<i>Mathews v. Eldridge</i> , 424 U.S. 319 (1976)	4, 5, 6, 13

<i>New York Times Co. v. United States</i> , 403 U.S. 713 (1971) (per curiam)	18
<i>Rafeedie v. INS</i> , 880 F.2d 506 (D.C. Cir. 1989)	4
<i>Rafeedie v. INS</i> , 795 F. Supp. 13 (D.D.C. 1992)	4
[Redacted], 2011 U.S. Dist. LEXIS 157706 (FISC Oct. 3, 2011)	12
<i>United States v. Andolschek</i> , 142 F.2d 503 (2d Cir. 1944)	20
<i>United States v. Aref</i> , 533 F.3d 72 (2d Cir. 2008)	15
<i>United States v. Daoud</i> , 755 F.3d 479 (7th Cir. 2014)	2, 9, 10
<i>United States v. James Daniel Good Real Property</i> , 510 U.S. 43 (1993)	6
<i>United States v. Gowadia</i> , 2010 U.S. Dist. LEXIS 80572 (D. Haw. May 8, 2010)	14
<i>United States v. Lee</i> , 79 F. Supp. 2d 1280 (D.N.M. 1999), <i>aff'd mem.</i> , 2000 U.S. App. LEXIS 3082 (10th Cir. Feb. 29, 2000)	19
<i>United States v. Lee</i> , 2000 U.S. App. LEXIS 3082 (10th Cir. Feb. 29, 2000)	16
<i>United States v. Progressive, Inc.</i> , 486 F. Supp. 5 (D. Wis.), <i>dismissed as moot</i> , 610 F.2d 819 (7th Cir. 1979)	18
<i>United States v. Reynolds</i> , 345 U.S. 1 (1953)	20
<i>United States v. Ruiz</i> , 536 U.S. 622 (2002)	5

<i>United States v. Yunis</i> , 867 F.2d 617 (D.C. Cir. 1989)	15
--	----

CONSTITUTION, STATUTES, AND RULES

U.S. Const. Amend. IV.....	<i>passim</i>
U.S. Const. Amend. V	<i>passim</i>
18 U.S.C. App. 3 § 3	14
18 U.S.C. App. 3 § 4	2, 8, 15
18 U.S.C. App. 3 § 9	14
18 U.S.C. § 3504	4
50 U.S.C. § 1806(f)	3, 13, 16
50 U.S.C. § 1806(g).....	4
Fed. R. Crim. P. 16	4

OTHER AUTHORITIES

S. Rep. 604(I), 95th Cong., 1st Sess., <i>reprinted in</i> 1978 U.S.C.C.A.N. 3904.....	20
S. Rep. 701, 95th Cong., 1st Sess., <i>reprinted in</i> 1978 U.S.C.C.A.N. 3973.....	20
Department of Justice, Office of Inspector General, <i>Annex to the Report on the President's Surveillance Program</i> (July 10, 2009).....	8
9 United States Attorney's Manual, Criminal Resource Manual § 2054(I)(C)	14
Al Weaver, <i>Paul Ryan: Nunes memo lays out a 'specific, legitimate' worry about surveillance</i> , Washington Examiner, Feb. 2, 2018	17

INTEREST OF AMICUS CURIAE

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the United States Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

NACDL has submitted amicus briefs in several cases involving the Foreign Intelligence Surveillance Act (FISA) and other government surveillance programs, including *Clapper v. Amnesty International USA*, 568 U.S. 598 (2013); *In re Sealed*

Case, 310 F.3d 717 (FISCR 2002); and *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 636 (2018).¹

All parties have consented to the filing of this brief.

SUMMARY OF THE ARGUMENT

In the 41 years since Congress enacted FISA, no court has ever ordered disclosure of the underlying applications, orders, and other materials.² And in those four decades, no court has ever ordered the fruits of FISA surveillance suppressed. Those remarkable facts are directly related. Without disclosure of the underlying FISA materials, it is impossible to argue under *Franks v. Delaware*, 438 U.S. 154 (1978), that the application contains material misstatements or omissions, and courts have no means of conducting the investigation necessary to make that determination themselves. Without disclosure, defendants cannot argue concretely that the government did not properly minimize the fruits of the surveillance, or that the government did not satisfy the requirement that it exhaust other, less intrusive investigative techniques before turning to FISA. Nor can defendants counter

¹ Counsel for amicus state that no counsel for a party authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting the brief; and no person other than amicus, its members, or its counsel made a monetary contribution to the preparation or submission of this brief.

² To be precise, one district court ordered disclosure and was promptly reversed on interlocutory appeal by the government. *United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014).

government arguments (typically presented *ex parte* under § 4 of the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3 § 4) that the fruits of particular surveillance techniques are too attenuated from the trial evidence to require disclosure. And without notice of particular surveillance techniques that the government used, a defendant cannot argue that, under the circumstances of the case, those techniques violate the Fourth Amendment or another constitutional or statutory protection.

As appellant argues, Congress never intended FISA litigation to occur entirely *ex parte*.³ Courts have misinterpreted 50 U.S.C. § 1806(f), the statute's disclosure provision. And as we discuss below, the Fifth Amendment Due Process Clause forbids such a secret, one-sided process, under which defendants are routinely denied the information necessary to challenge the lawfulness of government surveillance. No other aspect of criminal law functions entirely in secret; search warrants and Title III wiretap orders are issued *ex parte*, but after indictment a defendant gets access to the warrant or order and supporting application and a full and fair opportunity to challenge both. It is past time for FISA litigation to meet the standard of fairness that is the hallmark of American law.

³ Appellant's Opening Brief ("App. Br.") at 55-63.

ARGUMENT

The Fifth Amendment Due Process Clause requires disclosure of FISA applications, orders, and surveillance techniques in complex cases such as this, where disclosure is helpful to the defense in preparing a suppression motion.⁴ We analyze the due process issue under the three-part framework of *Mathews v. Eldridge*, 424 U.S. 319 (1976).⁵

Courts often turn to the *Mathews* balancing test to determine whether the government must disclose evidence it seeks to keep secret. *See, e.g., American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1068-71 (9th Cir. 1995) (applying *Mathews* test to determine whether use of secret evidence violates due process); *Rafeedie v. INS*, 880 F.2d 506, 524-25 (D.C. Cir. 1989) (*Mathews* balancing test governs process due alien in exclusion proceeding, including use of secret evidence), *on remand*, 795 F. Supp. 13, 18-20 (D.D.C. 1992) (same); *Kindhearts for Charitable Humanitarian Development, Inc. v. Geithner*, 710 F. Supp. 2d 637, 659 (N.D. Ohio 2010) ("Courts have found that their duty to protect

⁴ FISA itself directs the court to consider whether disclosure is required as a matter of due process. Section 1806(g) of Title 50 provides in relevant part that "[i]f 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.*" 50 U.S.C. § 1806(g) (emphasis added).

⁵ For the reasons stated in appellant's brief, amicus agrees that disclosure is also required under *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny, Fed. R. Crim. P. 16, and 18 U.S.C. § 3504.

individual rights extends to requiring disclosure of classified information to give a party an ability to respond to allegations made against it."); *Kiareldeen v. Reno*, 71 F. Supp. 2d 402, 413-14 (D.N.J. 1999) (same).⁶

Under *Mathews*, a court must weigh three factors to determine what process is due: (1) "the private interest that will be affected by the official action," (2) "the risk of an erroneous deprivation of such interest through the procedures used" and "the probable value, if any, of additional or substitute procedural safeguards," and (3) "the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirements would entail." 424 U.S. at 335. Application of the *Mathews* test confirms that, as a matter of due process, Muhtorov must be granted access to the FISA materials and notice of the surveillance techniques deployed against him.

I. MUHTOROV'S "PRIVATE INTEREST."

Muhtorov's "private interests" here are extremely weighty. He seeks an accurate determination of his claim that the government's secret surveillance violated his rights under FISA and the Fourth Amendment. He seeks to vindicate his constitutionally protected right to privacy. More generally, he seeks through the processes of the federal courts to avoid deprivation of his liberty. If mere property

⁶ Although these are civil cases, the Supreme Court has applied the *Mathews* test to determine the process due in criminal cases as well. *See United States v. Ruiz*, 536 U.S. 622, 631 (2002); *Ake v. Oklahoma*, 470 U.S. 68, 77 (1985).

interests "weigh heavily in the *Mathews* balance," as the Supreme Court has held, *United States v. James Daniel Good Real Property*, 510 U.S. 43, 54-55 (1993), Muhtorov's privacy and liberty interests have even greater significance.

II. THE RISK OF ERRONEOUS DEPRIVATION AND THE VALUE OF ADDITIONAL PROCEDURES.

Turning to the second *Mathews* factor, the adjudication of Muhtorov's rights under FISA and the Fourth Amendment through ex parte review of materials that his counsel had no opportunity to examine or challenge carries a notoriously significant "risk of an erroneous deprivation" of the liberty interests at issue, and "additional . . . procedural safeguards"--notice of the surveillance techniques used, access to the FISA materials, and an opportunity to address them--carry substantial "probable value." *Mathews*, 424 U.S. at 335. 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." *James Daniel Good*, 510 U.S. at 55 (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). As one court observed in a secret evidence case, "One would be hard pressed to design a procedure more likely to result in erroneous deprivations.' . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." *American-Arab Anti-*

Discrimination Committee, 70 F.3d at 1069 (quoting district court); *see, e.g., id.* at 1070 (noting "enormous risk of error" in use of secret evidence); *Kiareldeen*, 71 F. Supp. 2d at 412-14 (same).

In the Fourth Amendment context, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman v. United States*, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to its case against the defendants. The Court rejected the government's suggestion that the district court make that determination *ex parte* and *in camera*. The Court observed that

[a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Id. at 182. In ordering disclosure of improperly recorded conversations, the Court declared:

Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

Id. at 184.

Alderman remains a vital precedent. The government has often sought to keep surveillance techniques secret from the defense by arguing that the fruits of a particular technique are too attenuated from the evidence it seeks to use at trial to require disclosure. The government's position, usually presented in its *ex parte* submissions under CIPA § 4, is that the legality of the surveillance technique is irrelevant because the surveillance did contribute to the evidence the government will offer against the defendant at trial. *See* Department of Justice Office of Inspector General, *Annex to the Report on the President's Surveillance Program* at 347-51 (July 10, 2009) (describing this practice).⁷ But that is precisely the issue for which *Alderman* emphasized the importance of adversary proceedings.

In *Franks*, the Court highlighted another Fourth Amendment setting where adversary proceedings are necessary. The Court 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

⁷ The OIG Report is available at <https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf>.

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.

Franks recognizes that even with access to a search warrant and supporting affidavit, a defendant needs an evidentiary hearing to demonstrate that an affidavit contains intentional or reckless material falsehoods or omissions. A defendant seeking to make a *Franks* argument about a FISA application stands in an even worse position, because he lacks access either to the application itself or the resulting order. Without access to those materials, the defense can only speculate; it cannot identify specific falsehoods or omissions to make the "substantial preliminary showing" that *Franks* requires for an evidentiary hearing. *Id.* at 155-56. As Judge Rovner has acknowledged, "[I]t is well past time to recognize that it is virtually impossible for a FISA defendant to make the showing that *Franks* requires in order to convene an evidentiary hearing." *United States v. Daoud*, 755 F.3d 479, 496 (7th Cir. 2014) (Rovner, J., concurring). Judge Rovner added:

A *Franks* motion is premised on material misrepresentations and omissions in the warrant affidavit; but without access to that affidavit, a defendant cannot identify such misrepresentations or omissions, let alone establish that they were intentionally or recklessly made. As a practical matter, the secrecy shrouding the FISA process renders it

impossible for a defendant to meaningfully obtain relief under *Franks* absent a patent inconsistency in the FISA application itself or a *sua sponte* disclosure by the government that the FISA application contained a material misstatement or omission.

Id. at 486 (Rovner, J., concurring). The district court, lacking access to the discovery, to the information the defense possesses through its own knowledge and investigation, and to investigative resources, cannot assess on its own whether the applications contain falsehoods, or whether they omit information that would change the probable cause assessment. *See id.* ("[T]he court, which does have access to the application, cannot, for the most part, independently evaluate the accuracy of that application on its own without the defendant's knowledge of the underlying facts.").

Judge Rovner recognized that "*Franks* serves as an indispensable check on potential abuses of the warrant process, and means must be found to keep *Franks* from becoming a dead letter in the FISA context." *Id.* Those "means" are readily available here: provide defense counsel access to the FISA applications, orders, and other materials, as Congress intended and due process requires.

Notice of the *type* of surveillance is likewise necessary for a meaningful opportunity to challenge its legality. Although traditional FISA surveillance and "sneak and peek" searches remain investigative staples, the government has devised a series of other surveillance programs, including the section 702 program to which

Muhtorov was subjected,⁸ E.O. 12333, section 215 collection of financial and other records, cell site location information (CSLI), and so on. Some of those programs have become known through whistleblower disclosures, leaks, and congressional hearings.⁹ Others undoubtedly remain unknown. Almost every electronic device we interact with--from our phones to our cars to our refrigerators--transmits information about us. Absent notice, a defendant has no way knowing which of those devices the government may have surveilled, or by what technique. And without this information, the defendant cannot challenge the legality of the surveillance or demonstrate to the court how that surveillance contributed to the evidence the government seeks to introduce at trial.

In the absence of adversarial proceedings to test the legality of FISA surveillance, systematic executive branch misconduct--including submission of dozens of FISA applications with "erroneous statements" and "omissions of material facts"--went entirely undetected by the courts until the DOJ chose to reveal it. *See In re All Matters*, 218 F. Supp. 2d 611, 620-21 (FISC) (Lamberth, J.), *rev'd on other grounds*, 310 F.3d 717 (FISCR 2002). The FISC was sufficiently alarmed by these erroneous applications that it "decided not to accept inaccurate affidavits from FBI

⁸ Although Muhtorov received notice that he was subjected to section 702 surveillance, he was not informed specifically how the government obtained information about him under that program. App. Br. 57.

⁹ Appellant's brief lists several of the known surveillance programs. App. Br. 72-75.

agents whether or not intentionally false," and "[o]ne FBI agent was barred from appearing before the Court as a FISA affiant." *Id.* at 621.

These strong words apparently did not have their intended effect. In 2009, the FISC declared itself "deeply troubled" by incidents in which the NSA violated the court's orders. It noted that those incidents "occurred only a few weeks following the completion of an 'end to end review' by the government of NSA's procedures and processes for handling the BR metadata, and its submission of a report intended to assure the Court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems in this matter and had taken the necessary steps to ensure compliance with the Court's orders going forward." *In re FBI*, 2009 U.S. Dist. LEXIS 132935, at *4 (FISC Sept. 25, 2009) (Walton, J.). And again in 2011, the FISC was "troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program." *[Redacted]*, 2011 U.S. Dist. LEXIS 157706, at *20 n.14 (FISC Oct. 3, 2011) (Bates, J.). Of course, these are just the misrepresentations that came to the attention of the FISC and that the FISC chose to make public. It is impossible to know how many additional misrepresentations the FISC never learned about or elected to keep secret.

In light of the almost complete exclusion of criminal defendants and their counsel from the FISA process, and the correspondingly low risk that misconduct will be detected, it is understandable, if inexcusable, that officials "engaged in the often competitive enterprise of ferreting out crime," *Johnson v. United States*, 333 U.S. 10, 14 (1948), may have come to believe that FISA offers a convenient means of circumventing the traditional Title III and search warrant processes. The tendency of a secret, one-sided process to breed abuse underscores the need for disclosure and adversarial litigation when the government seeks to use FISA surveillance in a criminal case. The "additional . . . procedural safeguards" that Muhtorov requests--notice of the surveillance techniques deployed against him, access to the FISA materials, and an opportunity to address the legality of the surveillance in light of this information--thus carry substantial "probable value." *Mathews*, 424 U.S. at 335.

III. THE GOVERNMENT'S INTEREST.

Finally, the Court must consider the government's purported interest in maintaining the secrecy of the FISA materials and surveillance techniques.

The government invariably resists disclosure of FISA materials on the ground 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 when they

crafted the FISA disclosure provision, 50 U.S.C. § 1806(f). The argument is even more clearly wrong now, for two principal reasons.

First, through the use of "appropriate security procedures and protective orders," *id.*, a district court can order disclosure in a manner that adequately protects legitimate national security concerns. Such "security procedures and protective orders" are readily available following the enactment of the CIPA in 1980 (two years after FISA became law) and the extensive experience that courts, prosecutors, and defense counsel have had with the statute since then.

Most critically, CIPA provides for entry of a protective order.¹⁰ 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).¹¹ Although

¹⁰ 18 U.S.C. App. 3 § 3.

¹¹ 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.

the CSOs work for the Department of Justice, they are independent of the prosecution team. They advise the parties and the district 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.¹²

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 establishes the procedure for 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

¹² See 9 United States Attorney's Manual, Criminal Resource Manual § 2054(I)(C) (describing role of CSO).

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 § 4.¹³

CIPA has been in existence for 39 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 one case, for example, 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 at issue here. In short, CIPA provides precisely the "appropriate security procedures and protective orders" that

¹³ Nothing in CIPA affects the scope of the government's discovery obligations. As its name suggests, the statute is purely procedural. The government must produce any otherwise discoverable classified information (or a substitute that the district court finds to be adequate), as long as the information is "helpful" to the defense. *See, e.g., United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008); *United States v. Yunis*, 867 F.2d 617, 622-23 (D.C. Cir. 1989).

Congress contemplated would accompany disclosure when it enacted FISA. 50 U.S.C. § 1806(f).

Second, the government's "no disclosure ever to anyone" litigation position has been overtaken by events. On February 2, 2018, the President--head of the same Executive Branch that is prosecuting Muhtorov--declassified and approved release of a House Permanent Select Committee on Intelligence ("HPSCI") majority memorandum that summarized portions of a FISA application targeting an American citizen (Carter Page).¹⁴ According to the cover letter from the Counsel to the President, the President declassified the memorandum because "the public interest in disclosure outweighs any need to protect the information." The then-Speaker of the House of Representatives observed that release of the HPSCI memorandum "provide[s] greater transparency" concerning FISA and helps "ensure the FISA system works as intended and Americans' rights are properly safeguarded." Al Weaver, *Paul Ryan: Nunes memo lays out a 'specific, legitimate' worry about surveillance*, Washington Examiner, Feb. 2, 2018.

On February 24, 2018, HPSCI released a redacted, declassified version of a minority memorandum, which challenged certain assertions made in the majority

¹⁴ The HPSCI majority memorandum can be found at <https://docs.house.gov/meetings/IG/IG00/20180129/106822/HMTG-115-IG00-20180129-SD001.pdf>.

memorandum.¹⁵ The minority memorandum, like the majority memorandum, summarized portions of the underlying FISA application. In July 2018, redacted versions of the Page FISA applications and orders were disclosed to the New York Times through the FOIA process and were made public by the Times.¹⁶

The declassification and disclosure of the HPSCI memoranda and the redacted Page FISA materials demonstrate that it is possible to discuss publicly aspects of a FISA application without damaging national security. If the redacted Page FISA materials could be disclosed *publicly* without harming national security, as the Executive Branch determined, even more substantial disclosure of the Muhtorov FISA materials could be made to cleared defense counsel under the protections of CIPA without causing such harm.

The disclosure of the Page FISA materials, after years of government claims that any disclosure of FISA materials to any defense counsel ever would cause grave damage to national security, fits into a pattern of government exaggeration. In case after case over the years, the government has made national security claims that have proven overblown. To cite a few famous examples, the government argued in 1971 that disclosure of the Pentagon Papers would cause grave damage national security.

¹⁵ The HPSCI minority memorandum can be found at https://intelligence.house.gov/uploadedfiles/redacted_minority_memo_2.24.18.pdf.

¹⁶ The July 21, 2018 New York Times article describing the materials, with links to the redacted applications, can be found at <https://www.nytimes.com/2018/07/21/us/politics/carter-page-fisa.html>.

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 federal courts 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, 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 FISA materials are disclosed to cleared defense counsel in accordance with CIPA must be viewed skeptically, particularly following disclosure of the Page materials. 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. And if the government ultimately finds that risk unacceptable, then, as the Senate Judiciary and Intelligence Committees observed in enacting FISA, 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.

CONCLUSION

More than six decades ago, the Supreme Court declared that "since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material

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

Case No. 18-1366

I certify that pursuant to Fed. R. App. P. 29(a)(5) and 32(a), the foregoing brief is proportionately spaced, has a typeface of 14 points, and contains 4879 words.

/s/ John D. Cline
John D. Cline

ECF CERTIFICATE

U.S. Court of Appeals Docket Number: 18-1366

I hereby certify (1) that all privacy redactions have been made in the foregoing; (2) that the hard copy or copies of the foregoing that will be submitted to the Court is/are identical to the electronically filed version; and (3) that the foregoing has been scanned using the latest version of Sophos Antivirus for Mac Home Edition and no viruses or other threats were found.

/s/ John D. Cline
John D. Cline

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

U.S. Court of Appeals Docket Number: 18-1366

I hereby certify that on the 7th day of October 2019, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Tenth 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