

CASE 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
The Honorable John L. Kane, Senior U.S. District Judge
D.C. Case No. 1:12-cr-00033-JLK-1

APPELLANT’S OPENING BRIEF

PATRICK TOOMEY
ASHLEY GORSKI
American Civil Liberties Union
Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500

VIRGINIA L. GRADY
Federal Public Defender

JOHN C. ARCECI
Assistant Federal Public Defender
633 17th Street, Suite 1000
Denver, Colorado 80202
(303) 294-7002

Oral Argument is requested

September 30, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES	vi
PRIOR AND RELATED APPEALS	xvi
STATEMENT OF JURISDICTION.....	1
ISSUES PRESENTED.....	1
STATEMENT OF THE CASE.....	2
SUMMARY OF ARGUMENT	11
ARGUMENT	13
I. The government’s warrantless surveillance of Mr. Muhtorov was unconstitutional and the resulting evidence should be suppressed.	13
A. Preservation and standard of review.	15
B. The government relied on a novel surveillance statute, Section 702 of FISA, to seize and search Mr. Muhtorov’s communications without a warrant.	15
1. Section 702 dramatically expanded government surveillance under FISA by authorizing warrantless searches on U.S. soil.	16
2. The government uses Section 702 to amass Americans’ communications with more than 160,000 people abroad.	19
a. Breadth of the surveillance	20
b. Collection of Americans’ communications	22
c. “Backdoor searches” of Americans’ communications.....	24
3. The Section 702 surveillance of Mr. Muhtorov.	25

C.	The search and seizure of Mr. Muhtorov’s communications violated the Fourth Amendment’s warrant requirement.	27
1.	Section 702 permits surveillance of Americans’ international communications in violation of the warrant requirement.	28
2.	The government must obtain a warrant to search and use Americans’ communications regardless of whether it is “targeting” foreigners.....	29
3.	If there is a foreign-intelligence exception to the warrant requirement, it is not broad enough to render the surveillance of Mr. Muhtorov constitutional.	34
D.	The surveillance of Mr. Muhtorov violated the Fourth Amendment’s reasonableness requirement.....	36
1.	Section 702 surveillance lacks the core safeguards that courts require when assessing the reasonableness of electronic surveillance.	37
2.	The Section 702 procedures allow and encourage the warrantless exploitation of Americans’ communications, including through backdoor searches.	40
3.	The government has reasonable alternatives that would allow it to collect foreign intelligence while protecting Americans’ private communications.....	46
E.	The warrantless surveillance of Mr. Muhtorov violated Article III of the Constitution.....	47
F.	FISA mandates suppression when a court concludes that surveillance was unlawful.	51

II.	Given the novelty and complexity of the challenged surveillance, disclosure of the Section 702 and FISA materials was required.....	51
A.	Preservation and standard of review.	52
B.	Background and statutory framework.....	53
C.	Disclosure of the Section 702 and FISA materials was “necessary” for an accurate determination of the legality of the surveillance.....	55
1.	FISA’s text, structure, and legislative history confirm that disclosure is “necessary” in cases involving complex questions.....	55
2.	Mr. Muhtorov’s challenge involves significant legal, factual, and technological complexity.	56
D.	FISA must be construed to require disclosure consistent with the Fourth and Fifth Amendments.	63
E.	The government’s public disclosures belie its blanket claims of secrecy and require disclosure of comparable Section 702 and FISA materials here.....	66
III.	Beyond Section 702 and FISA, Mr. Muhtorov is entitled to notice of other novel surveillance tools used in the government’s investigation.....	69
A.	Preservation and standard of review.	70
B.	The government refused to disclose the novel surveillance tools, beyond Section 702 and FISA, used to investigate Mr. Muhtorov.....	71
C.	Recent decisions show that notice and adversarial litigation of Fourth Amendment questions is essential in an era of rapidly advancing technology.	76

D.	Mr. Muhtorov is entitled to notice of the government’s surveillance tools.....	77
1.	The Fourth and Fifth Amendments entitle Mr. Muhtorov to notice of the government’s surveillance techniques.	78
2.	18 U.S.C. § 3504 entitles Mr. Muhtorov to notice of the government’s surveillance techniques.	79
3.	The Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice of the government’s surveillance techniques.	80
E.	The government’s use of CIPA to conceal novel surveillance of Mr. Muhtorov violated both CIPA and due process.....	81
IV.	The nearly six-and-a-half-year delay between Mr. Muhtorov’s arrest and trial violated his constitutional right to a speedy trial.	88
A.	Preservation and standard of review	89
B.	The <i>Barker v. Wingo</i> factors overwhelmingly favor Mr. Muhtorov.....	89
1.	Length of the delay	89
2.	Reason for the delay	90
3.	Invocation of the right.....	92
4.	Prejudice	92
	CONCLUSION	97
	STATEMENT REGARDING ORAL ARGUMENT	97
	CERTIFICATES OF COMPLIANCE, DIGITAL SUBMISSION, AND SERVICE	99

ATTACHMENTS:

1. Judgment.
(V16 at 247-53)
2. District court's written ruling on Mr. Muhtorov's motion to suppress evidence resulting from Section 702 surveillance. (V3 at 115-49)
(Issue I)
3. District court's oral ruling on Mr. Muhtorov's same motion to suppress evidence resulting from Section 702 surveillance. (V11 at 264-67)
(Issue I)
4. District court's ruling on Mr. Muhtorov's challenge to government's withholding of traditional FISA materials. (V1 at 479-83)
(Issue II)
5. District court's ruling on Mr. Muhtorov's challenge to government's withholding of Section 702 materials. (V3 at 148-49)
(Issue II)
6. District court's oral ruling on Mr. Muhtorov's motion for notice of the government's surveillance techniques and objection to the government's use of Classified Information Procedures Act ("CIPA"). (V13 at 716)
(Issue III)
7. District court's oral ruling on Mr. Muhtorov's motion to dismiss for constitutional speedy trial violation. (V12 at 546-54)
(Issue IV)
8. District court's oral ruling on Mr. Muhtorov's renewed motion to dismiss for constitutional speedy trial violation. (V20 at 147-50)
(Issue IV)

TABLE OF AUTHORITIES

Cases

[Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)	<i>passim</i>
[Redacted], No. [Redacted] (FISC Apr. 26, 2017).....	25, 61
<i>ACLU v. Clapper</i> , 785 F.3d 787 (2d Cir. 2015)	57, 69, 77
<i>Aetna Life Ins. Co. v. Haworth</i> , 300 U.S. 227 (1937).....	48
<i>Alderman v. United States</i> , 394 U.S. 165 (1969).....	65, 78, 85, 86
<i>Barker v. Wingo</i> , 407 U.S. 514 (1972).....	89, 94
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	38, 39, 41, 78
<i>Brigham City v. Stuart</i> , 547 U.S. 398 (2006).....	37
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	45, 69, 74, 76
<i>Dalia v. United States</i> , 441 U.S. 238 (1979).....	28, 78
<i>Doggett v. United States</i> , 505 U.S. 647 (1992).....	92
<i>Ex parte Jackson</i> , 96 U.S. 727 (1877).....	34

Ferguson v. City of Charleston,
532 U.S. 67 (2001).....42

Flast v. Cohen,
392 U.S. 83 (1968).....48

Franks v. Delaware,
438 U.S. 154 (1978)..... 57, 59, 66

Hooper v. California,
155 U.S. 648 (1895).....63

In re All Matters Submitted to the FISC,
218 F. Supp. 2d 611 (FISC 2002).....61

In re Directives,
551 F.3d 1004 (FISCR 2008) 35, 40, 44

*In re Proceedings Required by § 702(i) of the FISA Amendments Act
of 2008*,
Misc. No. 08-01, 2008 WL 9487946 (FISC Aug. 27, 2008).....25

In re Sealed Case,
310 F.3d 717 (FISCR 2002) 35, 38, 41

In re Summers,
325 U.S. 561 (1945).....48

Jackson v. Ray,
390 F.3d 1254 (10th Cir. 2004).....95

Jencks v. United States,
353 U.S. 657 (1957).....78

Jones v. United States,
357 U.S. 493 (1958).....28

Katz v. United States,
389 U.S. 347 (1967)..... 27, 28, 38, 45

Keyes v. Sch. Dist. No. 1,
119 F.3d 1437 (10th Cir. 1997)49

Kolod v. United States,
390 U.S. 136 (1968).....86

Massachusetts v. EPA,
549 U.S. 497 (2007).....48

Mathews v. Eldridge,
424 U.S. 319 (1976).....65

Matter of Grand Jury,
524 F.2d 209 (10th Cir. 1975)80

McDonald v. United States,
335 U.S. 451 (1948).....38

Memorandum Opinion,
No. [Redacted], (FISC Aug. 30, 2013).....23

Muhtorov v. Choate,
697 F. App'x 608 (10th Cir. 2017)96

New Jersey v. T.L.O.,
469 U.S. 325 (1985).....34

New York v. Ferber,
458 U.S. 747 (1982).....48

Nolan v. United States,
423 F.2d 1031 (10th Cir. 1969)85

Riley v. California,
134 S. Ct. 2473 (2014)..... 29, 39, 59, 62

Rodriguez v. United States,
135 S. Ct. 1609 (2015).....42

Roviaro v. United States,
353 U.S. 53 (1957)..... 64, 68

Samson v. California,
547 U.S. 843 (2006).....37

Sec’y of State of Md. v. Joseph H. Munson Co.,
467 U.S. 947 (1984).....48

Smith v. Black,
904 F.2d 950 (5th Cir. 1990)64

Taglianetti v. United States,
394 U.S. 316 (1969).....85

Terry v. Ohio,
392 U.S. 1 (1968).....41

United States v. Alderisio,
424 F.2d 20 (10th Cir. 1970)86

United States v. Apple,
915 F.2d 899 (4th Cir. 1990) 79, 86

United States v. Aref,
533 F.3d 72 (2d Cir. 2008)84

United States v. Belfield,
692 F.2d 141 (D.C. Cir. 1982)..... 56, 60

United States v. Black,
830 F.3d 1099 (10th Cir. 2016)89

United States v. Bobo,
477 F.2d 974 (4th Cir. 1973)38

United States v. Carr,
939 F.2d 1442 (10th Cir. 1991)71

United States v. Chun,
503 F.2d 533 (9th Cir. 1974)84

United States v. Daoud,
755 F.3d 479 (7th Cir. 2014)66

United States v. Donovan,
429 U.S. 413 (1977)..... 30, 31, 40

United States v. Duggan,
743 F.2d 59 (2d Cir. 1984) 35, 38

United States v. Duka,
671 F.3d 329 (3d Cir. 2011)35

United States v. Figueroa,
757 F.2d 466 (2d Cir. 1985) 30, 31

United States v. Freitas,
800 F.2d 1451 (9th Cir. 1986)78

United States v. Frias,
893 F.3d 1268 (10th Cir. 2018)94

United States v. Gamez-Orduno,
235 F.3d 453 (9th Cir. 2000)63

United States v. Hanna,
661 F.3d 271 (6th Cir. 2011)81

United States v. Hasbajrami,
No. 17-2669 (2d Cir.)62

United States v. Kahn,
415 U.S. 143 (1974)..... 30, 31

United States v. Loera,
923 F.3d 907 (10th Cir. 2019)44

United States v. Lustyik,
833 F.3d 1263 (10th Cir. 2016)71

United States v. Medina,
918 F.3d 774 (10th Cir. 2019) 92, 95

United States v. Megahey,
553 F. Supp. 1180 (E.D.N.Y. 1982)49

United States v. Mesa-Rincon,
 911 F.2d 1433 (10th Cir. 1990) 38, 41

United States v. Mohamud,
 843 F.3d 420 (9th Cir. 2016)31

United States v. Place,
 462 U.S. 696 (1983).....42

United States v. Porter,
 745 F.3d 1035 (10th Cir. 2014)53

United States v. Ramsey,
 431 U.S. 606 (1977).....34

United States v. Renteria,
 720 F.3d 1245 (10th Cir. 2013)89

United States v. Rezaq,
 134 F.3d 1121 (D.C. Cir. 1998).....81

United States v. Sedaghaty,
 728 F.3d 885 (9th Cir. 2013) 29, 44, 84

United States v. Seltzer,
 595 F.3d 1170 (10th Cir. 2010)90

United States v. Soto-Zuniga,
 837 F.3d 992 (9th Cir. 2016)80

United States v. Soza,
 643 F.3d 1289 (10th Cir. 2011)15

United States v. Tigano,
 880 F.3d 602 (2d Cir. 2018)94

United States v. Tortorello,
 480 F.2d 764 (2d Cir. 1973) 38, 41

United States v. U.S. Dist. Court (Keith),
 407 U.S. 297 (1972)..... 27, 34, 78

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990)..... 32, 33

United States v. Villano,
529 F.2d 1046 (10th Cir. 1976)85

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 27, 45

Vermont v. New York,
417 U.S. 270 (1974).....49

Wong Sun v. United States,
371 U.S. 471 (1963)..... 60, 63

Statutes

18 U.S.C. § 2518.....34

18 U.S.C. § 32311

18 U.S.C. § 3504..... 79, 80

18 U.S.C. § 3742.....1

18 U.S.C. app. III..... *passim*

28 U.S.C. § 12911

50 U.S.C. § 1801 21, 44

50 U.S.C. § 1802.....44

50 U.S.C. § 1805 17, 18, 59

50 U.S.C. § 1806..... *passim*

50 U.S.C. § 1824.....59

50 U.S.C. § 1825 *passim*

50 U.S.C. § 186175

50 U.S.C. § 1881a *passim*

50 U.S.C. § 1881e52

FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.....16

Other Authorities

Affidavit of Admiral Michael Rogers, Director, NSA (July 2015).....67

Barton Gellman, Julie Tate, & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, Jul. 5, 2014.....22

Brief of Petitioner, *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013) (No. 11-1025).....16

Certification of DNI & Attorney General Pursuant to FISA Subsection 702(g) (July 2015).....67

Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013.....16

Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014 72, 73

David S. Kris & J. Douglas Wilson, *2 National Security Investigations & Prosecutions* (2d ed. 2012)..... 51, 79

DOJ Office of the Inspector General, *A Review of the Department of Justice’s Involvement with the President’s Surveillance Program* (July 2009)83

Elizabeth Goitein & Faiza Patel, *What Went Wrong with the FISA Court*, Brennan Center for Justice (Mar. 2015).....50

Elizabeth Goitein, *The Ninth Circuit’s Constitutional Detour in Mohamud*, Just Security (Dec. 8, 2016)31

Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case’s Undoing*, Wash. Post, Feb. 22, 201588

Executive Order 12,333 72, 73, 80

Executive Session, Committees on Judiciary and Government Reform
& Oversight, U.S. House of Representatives (Oct. 3, 2018).....72

FBI Section 702 Minimization Procedures (2015).....26

FBI Section 702 Targeting Procedures (2015)67

FBI Standard Minimization Procedures for FISA Electronic
Surveillance & Physical Search (2008)67

*Final Report of the S. Select Comm. to Study Governmental
Operations with Respect to Intelligence Activities (Book II),
S. Rep. No. 94-755 (1976).....17*

*FISA for the 21st Century: Hearing Before the S. Comm. on the
Judiciary, 109th Cong. (2006).....23*

*Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794,
H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on
Legis. of the H. Permanent Select Comm. on Intelligence,
95th Cong. (1978)50*

Geoffrey Stone & Michael Morell, *The One Change We Need to
Surveillance Law*, Wash. Post, Oct. 9, 2017.....43

Glenn Greenwald, *No Place to Hide* (2014).....21

H.R. 4870, 113th Cong. (2014).....47

In re Carter W. Page, Verified Application to the FISC (Oct. 2016)67

John Napier Tye, *Meet Executive Order 12333: The Reagan Rule
That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014.....72

John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up
Program Used to Investigate Americans*, Reuters, Aug. 5, 2013.....88

NSA Section 702 Minimization Procedures (2011) 25, 67

NSA Slides Explain the PRISM Data-Collection Program,
 Wash. Post, Jun. 6, 201320

Office of the Dir. of Nat’l Intelligence, *2018 Statistical Transparency Report* (2019) 18, 21

Office of the Dir. of Nat’l Intelligence, *IC on the Record*.....67

Order, *In re Prod. of Tangible Things From [Redacted]*,
 No. BR 08-13 (FISC Mar. 2, 2009)75

Orin Kerr, *The Surprisingly Weak Reasoning of Mohamud*, *Lawfare*
 (Dec. 23, 2016) 31, 32, 62

Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, *Lawfare* (Oct. 19, 2017)43

President’s Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (2013) 30, 47

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

Ryan Gallagher, *The Surveillance Engine*, *Intercept*, Aug. 25, 2014.....73

S. Rep. No. 701, 95th Cong., 2d Sess., *reprinted in*
 1978 U.S.C.C.A.N. 403356

S.A. 3979, 110th Cong. (2008), 154 Cong. Rec. S607–08
 (daily ed. Feb. 4, 2008)46

Secondary Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc.*, No. BR 13-80 (FISC Apr. 25, 2013)75

Two Sets of Rules for Surveillance, *N.Y. Times*, Aug. 13, 2014.....73

Rules

Federal Rule of Criminal Procedure 1680

Federal Rule of Appellate Procedure 4.....1

Federal Rule of Appellate Procedure 28.....89

PRIOR AND RELATED APPEALS

Mr. Muhtorov’s appeal is procedurally consolidated with that of his co-defendant, Bakhtiyor Jumaev (18-1296). *See* Order, Oct. 1, 2018.

This Court previously has considered two appeals related to this case: (1) a bond appeal filed by the government (17-1220); and (2) a pro se 28 U.S.C. § 2241 appeal filed by Mr. Muhtorov (17-1252).

STATEMENT OF JURISDICTION

The district court had jurisdiction over this criminal case under 18 U.S.C. § 3231. It entered judgment on September 4, 2018. V16 at 247.¹ Mr. Muhtorov timely appealed on September 7, 2018. *Id.* at 254. This Court has appellate jurisdiction under 18 U.S.C. § 3742(a) and 28 U.S.C. § 1291.

ISSUES PRESENTED

I. Whether the government’s warrantless surveillance of Mr. Muhtorov under Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) was unconstitutional?

II. Whether, given the novelty and complexity of the challenged surveillance, disclosure to Mr. Muhtorov of the underlying Section 702 and FISA materials was required for litigation of his suppression motions?

III. Whether Mr. Muhtorov is entitled to notice of other novel surveillance tools used in the government’s investigation and the opportunity to seek suppression?

IV. Whether the over six-year delay between Mr. Muhtorov’s arrest and trial violated his constitutional speedy trial right?

¹ Citations are to the volume (“V”) of the appellate record and the page number at the bottom right-hand side of each page.

STATEMENT OF THE CASE

A. Fleeing persecution for his human rights work in Uzbekistan, Mr. Muhtorov becomes a refugee in the United States.

Jamshid Muhtorov's story begins a world away in the Central Asian country of Uzbekistan. He grew up under two oppressive regimes, first the Soviets, and then, after the collapse of the Soviet Union, a brutal dictator named Islam Karimov who ruled the newly independent country for decades. V11 at 1020-28; V12 at 238.

Under Karimov, Uzbekistan was, in the words of one regional expert, "by far one of the worst and most repressive situations of human rights on earth." V20 at 299, 1312, 1402-10. The government stamped out free expression, imprisoned thousands of people on false charges, tortured detainees, and subjugated the country's Muslim population under some of the world's most restrictive laws governing religion. V20 at 299, 1312-1323, 1407-15.

It was in this environment that Mr. Muhtorov chose to work as a human rights activist. He led a regional branch of Ezgulik, the country's only human rights organization, and became "one of the more prominent and reputable human rights defenders in the country." V20 at 1313, 1321, 1411. But what little tolerance the Karimov regime showed for dissent collapsed in 2005, after government troops opened fire on a peaceful protest in the city of Andijan, killing hundreds. Mr.

Muhtorov and others spoke out against the government, and publicized the massacre with international media. V20 at 1415.

The regime's response was predictable—it cracked down harder, repressing journalists and jailing dissenters. V20 at 1315-17, 1415-20. Mr. Muhtorov was beaten on two occasions; the second time left for dead, bloodied, battered, and unconscious in the street. His mother and brother lost their government jobs; his sister and father were arrested on specious charges. V16 at 210.

Eventually he had to flee. Smuggled out of the country disguised as a woman, he joined other Uzbek refugees across the border in neighboring Kyrgyzstan. V16 at 94. His wife and two young children joined him, and they began a life in refuge. V16 at 210; V20 at 1108, 1272.

But national borders are often porous in that part of the world, and kidnappings by the Uzbek secret police routinely occurred even in neighboring countries. V20 at 1317-24, 1418-21. A documentary filmmaker working amongst the refugees got wind that Mr. Muhtorov's capture was imminent and helped him flee again, deeper into Kyrgyzstan. V20 at 1324-28.

In 2007, Mr. Muhtorov and his family were granted admission to the United States as political refugees. V16 at 210. They settled in Denver, Colorado, and became lawful permanent residents of the country. V1 at 669; V18 at 455.

B. Mr. Muhtorov assimilates to life in America, where for the first time he can speak freely, read freely, and practice his faith freely.

Mr. Muhtorov and his wife soon found work; her as a hotel housekeeper, him as a janitor, emptying ashtrays in mountain casinos and cleaning slaughterhouse floors. V20 at 1150, 1340. In search of better pay, he decided to get his commercial trucker's license, which is how he first crossed paths with co-defendant Bakhtiyor Jumaev. V16 at 211.

Mr. Jumaev was a fellow Uzbek exile living in Philadelphia, a city with one of the few trucking classes offered in Russian (which Mr. Muhtorov spoke from Soviet days). V20 at 1274. In late 2009, a friend arranged for Mr. Muhtorov to stay in Mr. Jumaev's apartment while he sought his trucking license. V16 at 210-11.

The two men had similar backgrounds. Both left Uzbekistan at the hands of government brutality, and, like most Uzbeks, both were Muslim. *Id.* They became friendly, and after Mr. Muhtorov returned to Colorado, they talked frequently on the phone. *Id.* When immigration agents arrested Mr. Jumaev the following year for visa violations, Mr. Muhtorov contributed \$500 to his bond. *Id.*; V20 at 1154. Mr. Jumaev's efforts to pay that money back would, years later, form a central part of this case.

In the United States, Mr. Muhtorov experienced freedoms he'd never known before. For the first time, he began to learn about and practice his family's Islamic faith. V20 at 1073-75, 1284. And like many refugees from repressive regimes, he

had a thirst for unfiltered news, and scoured the internet for information about the situation in his homeland. V11 at 1075-76; V12 at 310.

Mr. Muhtorov got his trucking license, and drove long-haul routes across America. V20 at 397; V16 at 96. Over the long hours on the road, he was eager to converse with others about all he was learning. V16 at 205. A self-described braggart, who the district court observed “craved attention and admiration from others,” he shared his views often. V16 at 208. Indeed, as the evidence at trial showed, Mr. Muhtorov talked, and talked, and talked some more—to anyone who would listen, and to some he didn’t know were listening.

C. The U.S. government begins surveilling Mr. Muhtorov shortly after his resettlement, ultimately monitoring nearly every facet of his life.

We don’t know precisely when the United States government began surveilling Mr. Muhtorov. Like much in this case, the government has shielded that information behind a veil of classification. V12 at 755; V13 at 405, 581-82; V20 at 660-63, 694. But every indication suggests it wasn’t too long after his arrival in the country. V11 at 483-87, 695-98; V12 at 356-59, 406-08, 549; V13 at 456-61.

Its efforts were all-encompassing. Over the years, federal agents tracked Mr. Muhtorov’s comings and goings. V11 at 512; V20 at 659, 717-18. They installed bugs in his home, listening to the intimate details of his family life. V3 at 604-05; V20 at 233. They recorded and listened to his phone calls, with Mr. Jumaev and

others, often long conversations about family, faith, and the mundanities of everyday life. V1 at 180-86; V12 at 824; V16 at 211. And, utilizing clandestine surveillance tools of unprecedented scope, they intercepted untold amounts of his electronic communications. *Infra* Parts I & II. Other tools the government employed remain secret to Mr. Muhtorov to this day. *Infra* Part III. And throughout all this, agents nicknamed him “Borat,” after the caricature of a bumbling reporter from Kazakhstan popular at the time. V20 at 657.

Although the government apparently monitored Mr. Muhtorov for years, what ultimately led to the charges in this case were Mr. Muhtorov’s communications about, and with, an Uzbek militant group named the Islamic Jihad Union.

The Karimov regime prompted two types of opposition—some dissidents, like Mr. Muhtorov, became activists; others formed violent opposition groups to topple the government, the most prominent of which was the Islamic Movement of Uzbekistan (“IMU”). V16 at 209; V12 at 241-42. The IMU splintered in 2001, when some members founded the offshoot Islamic Jihad Union (“IJU”). V20 at 311-12. The IJU shared the IMU’s goal of regime change in Uzbekistan, but also committed itself to a broader vision of Islamic rule. V20 at 307, 312, 325-256, 345-52. Throughout the 2000s, the IJU was implicated in attacks on Western targets in the region and coalition troops in Afghanistan. Although it boasted

hundreds of members in its heyday, by the decade's end, its numbers had dwindled dramatically. V20 at 296, 305-06, 314; V16 at 209-10. Both the IMU and IJU are designated as terrorist organizations by the U.S. government. V18 at 442.

The IJU maintained an Uzbek-language website, Sodiqlar.com, where it posted news from the region and propaganda, and used an email account to correspond with people worldwide. V20 at 317, 379. Mr. Muhtorov began visiting the website as he searched for information about his homeland, and throughout at least 2011, emailed periodically with individuals who helped operate the site. V16 at 211; V20 at 399, 1192-94, 1227-28. In these messages, he expressed support for the IJU's cause, and at times offered help with things like finding communications technology the group could use or posting its videos to YouTube, although he lacked the skills to personally accomplish either task. V16 at 122; V20 at 412-39. At one point, he sought to make an "oath" of allegiance to the organization, an offer the IJU met with silence. V16 at 97.

Mr. Muhtorov later explained that he corresponded with the group to learn more about the situation in Uzbekistan and their plans to overthrow Karimov, whom he saw as a common enemy. V20 at 1197-2101, 1213, 1244. His messages and offers were a way to build trust, and simply a fictional persona. V20 at 1192-94. The IJU itself recognized this in large measure, noting that Mr. Muhtorov's "main goal was to overturn the existing totalitarian regime in Uzbekistan and to

free Muslim people, suffering under this regime,” and that they had viewed him with suspicion and kept him at arm’s length. V20 at 344-45, 369.

Throughout 2011, Mr. Muhtorov also spoke extensively to Mr. Jumaev. They talked about their families, faith, and current events. They also conversed about the IJU and IMU, and jihadist videos they found online. They often used “code words” to discuss these topics, albeit ones widely known. V12 at 275-77, 288; V16 at 211-12; V20 at 333. Mr. Muhtorov shared with Mr. Jumaev that he’d had contact with the IJU, although, with characteristic braggadocio, often overstated those interactions. V20 at 632-33, 1186-89.

In Uzbek culture, one doesn’t talk directly about money, so Mr. Muhtorov often hinted about his financial struggles to remind Mr. Jumaev of the debt still owed. V20 at 1167, 1221, 1230-32. He also talked about how the IJU had told him it was in need of financial support. V16 at 212.

In March 2011, Mr. Jumaev sent a check for \$300 to Mr. Muhtorov. The men sometimes talked about the money as a “wedding gift,” a not-so-secret “code word” for aid to the IJU’s jihadist efforts. V16 at 212; V20 at 1029. But when the check arrived, Mr. Muhtorov’s wife cashed it and spent the money on groceries. V20 at 239, 457, 1293-94. Nonetheless, Mr. Muhtorov would still sometimes tell people that he’d received the money as a “wedding gift,” and he told the IJU the same, although the group never accepted this “gift.” V16 at 212; V20 at 590-94.

Late in 2011, Mr. Muhtorov began planning a trip to Turkey. His parents were urging him to help one of his brothers, who was trapped in a Kazakhstan refugee camp, get asylum elsewhere. V20 at 1276, 1296, 1357. Istanbul is a hub for travel to Central Asia, and also home to a U.N. refugee office and a religious school that Mr. Muhtorov was interested in attending. V20 at 360, 1159-68, 1420-27. So Mr. Muhtorov thought he could accomplish a lot by traveling there. V16 at 97; V20 at 1164-71.

But as the district court recognized, Mr. Muhtorov “told countless contradictory stories about the length, destination, and purpose of his trip to every listening ear he could find.” V16 at 213. The government listened to them all. V20 at 397. And in some of those stories—told to Mr. Jumaev and to a government informant pretending to be a jihadist sympathizer who might help Mr. Muhtorov’s brother settle in Germany—he indicated that he’d travel on from Turkey to join the IJU. V20 at 736; V21 at 23-62, 69, 82-85. This was despite the fact that the IJU had never accepted him, let alone offered instructions on how to find them thousands of miles and across a warzone from Istanbul. V16 at 97; V20 at 364, 380.

But when Mr. Muhtorov went to board his flight on January 21, 2012, federal agents arrested him at the airport, and accused him of attempting to travel overseas to provide support to the IJU. V20 at 396-400.

D. The government charges Mr. Muhtorov, and later Mr. Jumaev, with trying to support terrorism, and then takes more than six years to bring the men to trial.

Although he was arrested in January 2012, the government didn't bring Mr. Muhtorov to trial until May 2018. He was detained that entire time. V16 at 230; V19 at 438. Mr. Jumaev, who was arrested a few months later, fared similarly, and wasn't tried until March 2018.

Needless to say, a lot happened during those six-and-a-half years. Much of it is recounted in Mr. Jumaev's briefing, and, where pertinent, additional facts are discussed below.

Ultimately, a jury convicted Mr. Muhtorov of three counts alleging that he'd tried to provide material support to a foreign terrorist organization, all violations of 18 U.S.C. § 2339B: (1) conspiring, and (2) attempting to provide the \$300 from Mr. Jumaev to the IJU, and (3) attempting to provide himself as personnel to that group. V15 at 575-76. It acquitted on a fourth material-support count. V16 at 208. In a separate trial, Mr. Jumaev also was found guilty of the first two counts. *Id.*

The district court sentenced Mr. Muhtorov to eleven total years' incarceration.² V20 at 1673. This appeal follows.

² Given the length of his pretrial detention, he is expected to complete that sentence in September 2021.

SUMMARY OF ARGUMENT

The government's prosecution of Mr. Muhtorov relied on an unprecedented—and unconstitutional—form of electronic surveillance. This surveillance, conducted under Section 702 of FISA, is unlike anything this Court has countenanced, and it violated the Fourth Amendment's warrant and reasonableness requirements, as well as Article III of the Constitution. Because of this, the district court erred in denying Mr. Muhtorov's suppression motion.

Additionally, Mr. Muhtorov's entire suppression litigation was undercut by the government's refusal to disclose *any* of the underlying materials related to its Section 702 and other FISA-based surveillance. The district court declined to order the government to disclose this critical information, a decision that was erroneous because that disclosure was required as a matter of constitutional and statutory law.

The district court also erred by failing to require the government to disclose its use of still *other* warrantless surveillance tools to investigate Mr. Muhtorov—including novel technologies that courts have since found unlawful. In the absence of notice, Mr. Muhtorov had no meaningful opportunity to seek suppression of the fruits of this surveillance. But he was entitled to such notice under the Constitution, statutory law, and the federal rules, and the government's use of classified proceedings to litigate suppression issues in secret violated Mr. Muhtorov's right to adversarial process.

Each of these challenges presents questions of first impression in this Circuit, and each requires a remand to the district court for further proceedings.

Finally, and alternatively, Mr. Muhtorov also joins, under Fed. R. App. P. 28(i), in co-defendant Mr. Jumaev's constitutional speedy trial challenge. The over six-and-a-half-year delay between Mr. Muhtorov's arrest and trial violated his Sixth Amendment rights and dismissal of the indictment is warranted.

ARGUMENT

I. The government’s warrantless surveillance of Mr. Muhtorov was unconstitutional and the resulting evidence should be suppressed.

This case involves a novel kind of electronic surveillance, one unlike anything this Court has countenanced in the past. Relying on a law known as Section 702 of FISA, 50 U.S.C. § 1881a, the government intercepts billions of international communications sent by hundreds of thousands of individuals, including Americans. The government stores these communications in massive databases, retains them for years, and searches them repeatedly for information about Americans—including in domestic criminal investigations. This surveillance takes place inside the United States and with only limited involvement by judges on the Foreign Intelligence Surveillance Court (“FISC”). All of this surveillance is conducted without a warrant.

Mr. Muhtorov was one of the many Americans whose private communications have been vacuumed up, pooled together in government databases, and then examined by FBI agents without any judicial finding of probable cause. This surveillance violated the Constitution.

Section 702 surveillance, including the surveillance of Mr. Muhtorov here, lacks safeguards for Americans that the Constitution requires. Indeed, there is a profound mismatch between the government’s justification for this warrantless surveillance and the way it actually uses the wealth of private emails and phone

calls it obtains. Under Section 702, the government claims to “target” foreigners abroad who lack Fourth Amendment rights. Yet this surveillance routinely sweeps up Americans whose communications are indisputably entitled to constitutional protection. Rather than discarding Americans’ communications or tightly restricting their use—given the absence of a warrant—the government exploits this loophole. It amasses the communications it collects under Section 702 in databases available to FBI agents around the country, who deliberately perform searches for the communications of Americans. In short, no warrant ever stands between investigators and these protected communications. Even if the Constitution permits the government to target foreigners abroad, it does not permit this end-run around Americans’ Fourth Amendment rights.

This surveillance also violates Article III. Under Section 702, the government asks the FISC to issue mass surveillance orders—resulting in the routine collection of Americans’ communications—without any concrete factual showing. Because the statute requires judges to issue advisory opinions on broad legal questions in the absence of any “case or controversy,” the surveillance of Mr. Muhtorov was unconstitutional.

While Section 702 surveillance suffers from several constitutional defects, there is a narrow way for the Court to resolve the challenge here: by finding that the procedures governing the surveillance of Mr. Muhtorov were constitutionally

unreasonable, and thus violated the Fourth Amendment, because they permitted agents to freely use and search for the communications of Americans without a warrant. The procedures failed to require individualized judicial approval at any point—even after the fact, and even when the government sought to use or query the communications of a *known* U.S. person. It may well be that the government can adopt constitutionally sound procedures going forward, but this Court should find the procedures used to surveil Mr. Muhtorov defective.

A. Preservation and standard of review.

Mr. Muhtorov’s challenge to the Section 702 surveillance of his communications was raised and ruled on below. V1 at 666 (motion to suppress); V3 at 115 (order denying); V11 at 264-67 (oral ruling). This Court reviews *de novo* the legal questions of whether that surveillance violated the Fourth Amendment and Article III of the Constitution. *See United States v. Soza*, 643 F.3d 1289, 1291 (10th Cir. 2011).

B. The government relied on a novel surveillance statute, Section 702 of FISA, to seize and search Mr. Muhtorov’s communications without a warrant.

Mr. Muhtorov’s prosecution is the first case in the country in which the government acknowledged using Section 702. V1 at 552 (notice). Although the government collects billions of communications under this statute, for years it thwarted legal challenges by wrongly concealing its use of Section 702

surveillance. The Solicitor General even informed the Supreme Court that prosecutors would notify defendants of the surveillance, when in fact, unbeknownst to him, the Department of Justice had a practice of hiding the use of Section 702 in criminal cases. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, <https://nyti.ms/2NmNFpS>; Pet. Br. at 8, *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013) (No. 11-1025). Mr. Muhtorov learned of the warrantless surveillance in this case only after the government’s misrepresentations came to light.

1. Section 702 dramatically expanded government surveillance under FISA by authorizing warrantless searches on U.S. soil.

Section 702, codified by the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, revolutionized—and dramatically expanded—the government’s surveillance powers. The statute “creat[ed] a new framework” under which the government could obtain broad authorizations from the FISC to conduct warrantless surveillance targeting the communications of non-U.S. persons located abroad. *Amnesty*, 568 U.S. at 404. In the course of this surveillance, the government routinely obtains the communications of Americans like Mr. Muhtorov.

This new framework represented a stark departure from FISA’s original design and the protections it afforded Americans. In 1975, Congress established a

committee, chaired by Senator Frank Church, to investigate allegations of “substantial wrongdoing” by federal intelligence agencies. *Final Report of the Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II)*, S. Rep. No. 94-755, at v (1976) (“Church Report”). The committee discovered that, over the course of decades, the intelligence agencies had “infringed the constitutional rights of American citizens” and “intentionally disregarded” legal limitations on surveillance in the name of “national security.” *Id.* at 137. Of particular concern to the committee was that the agencies had “pursued a ‘vacuum cleaner’ approach to intelligence collection,” in some cases intercepting Americans’ communications under the pretext of targeting foreigners. *Id.* at 165. To ensure the protection of Americans’ communications, the committee recommended that all surveillance of communications “to, from, or about an American without his consent” be subject to a judicial warrant procedure. *Id.* at 309.

In 1978, largely in response to the Church Report, Congress enacted FISA to impose safeguards against warrantless surveillance of Americans. In its original form, FISA generally required the government to obtain individualized judicial approval of each person it sought to target. *See* 50 U.S.C. § 1805. The statute created a secret Article III court, the FISC, and authorized surveillance only after a FISC judge found “probable cause” that each target was a “foreign power” or the

“agent of a foreign power.” *Id.* § 1805(a)(2)(A)–(B). Thus, the government generally could not intercept phone calls or emails inside the United States, even for foreign-intelligence purposes, unless it first made a showing of individualized suspicion before a neutral magistrate.

Section 702 significantly altered this regime by abandoning these core requirements. Like surveillance under FISA, Section 702 surveillance takes place on U.S. soil. But under Section 702, surveillance occurs without any finding of probable cause or showing of individualized suspicion. 50 U.S.C. § 1881a. The government need not demonstrate to any court that the people it seeks to surveil are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Instead, Section 702 permits the government to target *any* foreigner located outside the United States to obtain foreign-intelligence information. *Id.* § 1881a(a). Moreover, the resulting surveillance does not sweep up *only* foreigners. Rather, the statute allows the government to warrantlessly obtain every phone call, email, video chat, or instant message between an American and the more than 160,000 foreigners who are targeted.³

While the statute is complex, its purpose and effect are straightforward: to permit the broad surveillance of digital communications entering and leaving the

³ See Office of the Dir. of Nat'l Intelligence (“ODNI”), *2018 Statistical Transparency Report* 13 (2019), <https://bit.ly/30EzXCO>.

United States, with only limited court involvement. Court review occurs just once a year, as follows. On an annual basis, the Attorney General and Director of National Intelligence issue a broad authorization permitting the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information,” together with “targeting” and “minimization” procedures. 50 U.S.C. § 1881a(a), (d)–(h). The FISC’s role consists principally of reviewing these general rules that the government proposes to use in carrying out the surveillance. *Id.* § 1881a(j). The government need not ever inform the FISC whom it intends to target or on what factual basis. And, critically, the government need not even seek a warrant when its agents decide to peruse the communications of Americans swept up in this surveillance. Instead, agents have wide latitude to sift through the communications pulled in under Section 702—including in the course of investigating Americans.

2. The government uses Section 702 to amass Americans’ communications with more than 160,000 people abroad.

The surveillance of Mr. Muhtorov can be understood only within the government’s broader implementation of Section 702. Several aspects of this surveillance bear emphasis. First, Section 702 surveillance is vast in scope. Second, it purposefully sweeps up the international communications of Americans without a warrant. And third, the “minimization” procedures that are supposed to protect the privacy of Americans in fact do the opposite: by allowing the

government to amass Americans' communications in databases where agents can later examine them for virtually any investigative purpose.

a. Breadth of the surveillance

Section 702 surveillance is incredibly broad. The government “targets” more than 160,000 people overseas and, in so doing, sweeps in billions of electronic communications, including Americans' communications. The government carries out this surveillance inside the United States with the cooperation of major American telecommunication and internet companies. Section 702 reaches every form of modern electronic communication: telephone calls, emails, video calls, texts, and online chats, among others.⁴

The government conducts Section 702 surveillance in at least two ways, commonly known as PRISM and Upstream. Under PRISM, the government directs internet service providers, such as Google and Facebook, to turn over the communications of their users. Under Upstream, the government cooperates with telecommunication companies, like AT&T and Verizon, to search communications in bulk as they flow through internet backbone cables. *See Privacy & Civil Liberties Oversight Board, Report on the Surveillance Program Operated*

⁴ *NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post, Jun. 6, 2013, <http://wapo.st/J2gkLY>.

Pursuant to Section 702 at 7 (2014), <https://perma.cc/WD5R-5GKE> (“PCLOB Report”).

The latitude afforded by the statute facilitates sweeping collection. The government can target *any* foreigner abroad to obtain “foreign intelligence information”—a term broadly defined to encompass nearly any information bearing on the foreign affairs of the United States. 50 U.S.C. § 1801(e). Using this authority, the government reported that, in 2018, it monitored the communications of 164,770 targets under a single mass surveillance order.⁵ In 2011, when it monitored approximately one-third that number of targets,⁶ the government still collected more than 250 million communications.⁷ Today, with nearly three times as many targets, the government likely collects over a billion communications under Section 702 each year. PCLOB Report 116 (noting the “current number is significantly higher” than in 2011).

Although the government targets a significant number of persons under Section 702, the number of “targets” does not reflect the true scope of the surveillance. The *Washington Post*’s review of a “large cache of intercepted

⁵ ODNI, *2018 Statistical Transparency Report* 13, <https://bit.ly/30EzXCO>.

⁶ Glenn Greenwald, *No Place to Hide* 111 (2014), <https://perma.cc/6VU2-5RNH> (NSA documents showing that 35,000 “unique selectors” were surveilled under PRISM in 2011).

⁷ [Redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

conversations” revealed that the vast majority of people subject to surveillance “were not the intended surveillance targets but were caught in a net the agency had cast for somebody else.” Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, Jul. 5, 2014, <http://wapo.st/1MVootx>. The material reviewed by the *Post* consisted of 160,000 intercepted email and instant message conversations, 7,900 documents—including “medical records sent from one family member to another, resumes from job hunters and academic transcripts of schoolchildren”—and more than 5,000 private photos. *Id.* The *Post* estimated that the government’s annual collection under Section 702 would give agents access to the communications of more than 900,000 people. *Id.*

b. Collection of Americans’ communications

This sprawling surveillance apparatus inevitably—and intentionally—sweeps in the communications of Americans without a warrant. As the FISC has observed, Section 702 surveillance results in the government obtaining “substantial quantities of information concerning United States persons and persons located inside the United States who are entitled to Fourth Amendment protection.”⁸

⁸ [Redacted] at 24 (FISC Aug. 30, 2013), <https://perma.cc/GR62-FNQC>.

Indeed, intelligence officials have stated that this is one of the principal aims of the surveillance.⁹

Each time an American communicates with any one of the government's targets—which may include journalists, academics, human rights researchers, or employees of foreign-owned corporations—the government collects and stores that communication. It is unknown precisely how many Americans are swept up in the government's surveillance web. Despite repeated requests from members of Congress, the government has refused even to estimate the number of Americans' communications it collects under Section 702. By all accounts, however, the volume is significant. *See* PCLOB Report 114.

Critically, the billions of communications intercepted under Section 702 are far too great in number for government analysts to review individually, let alone use. Thus, there is no “minimization” of Americans' emails and phone calls at the moment the communications are obtained. They are simply added to the government's massive databases of intercepted communications, to await later search, use, and analysis. PCLOB Report 128-29.

⁹ *See FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 9 (2006), <https://bit.ly/2ZwmOOH> (statement of NSA Director Michael Hayden).

c. “Backdoor searches” of Americans’ communications

Not only are Americans’ communications collected in substantial quantities, they are also retained, searched, and used in later investigations—including in domestic criminal investigations unrelated to the foreign-intelligence purpose for which they were ostensibly collected. *See* PCLOB Report 59. The government stores the collected communications in long-term databases, where agents routinely search through them—including by using Americans’ names or email addresses to investigate particular Americans. *See id.* at 58-60. These “backdoor searches” allow the government to target and read the communications of Americans without obtaining a warrant or any specific judicial authorization. In short, these warrantless queries are designed to extract communications that the government *knows* are protected by the Fourth Amendment.

Section 702’s “targeting” and “minimization” procedures fail to cure the dramatic invasions of privacy worked by the surveillance.

These rules, which supposedly protect the privacy of Americans swept up in the government’s surveillance apparatus, are weak by design. By default, they permit the government to keep virtually *all* communications collected under PRISM for as long as five years. During that time, agents can search and review the emails of foreigners and Americans alike without meaningful restriction. Beyond this initial five-year period, the minimization procedures explicitly permit

the government to retain and disseminate Americans’ international communications for almost a dozen reasons, including when it determines that the communications contain “significant foreign intelligence information” or “evidence of a crime.” *See* NSA Section 702 Minimization Procedures §§ 3(b)(2), 3(c)(1), 5(1)-(2), 6(a)(2), 6(b) (2011), <https://bit.ly/2KL3Bzp>. The procedures do not require a warrant—or even high-level executive-branch approval—before agents can go looking for an American’s private emails or phone calls. PCLOB Report 58-59 (discussing FBI procedures).

The FISC’s review of the targeting and minimization procedures does not remedy their deficiencies. As the FISC itself has noted, its review under the statute is “narrowly circumscribed” and is conducted only once a year.¹⁰ Those proceedings are typically one-sided and, by the FISC’s own description, have been plagued by an “institutional lack of candor” by the government.¹¹

3. The Section 702 surveillance of Mr. Muhtorov.

The government has acknowledged that it used Section 702 surveillance to obtain Mr. Muhtorov’s communications. V1 at 552. Based on the available evidence, it is also clear that FBI agents subjected Mr. Muhtorov to backdoor

¹⁰ *In re Proceedings Required by § 702(i) of FISA Amendments Act*, Misc. No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008).

¹¹ [Redacted] at 19 (FISC Apr. 26, 2017), <https://perma.cc/7X2S-VAS7> (“April 26, 2017 FISC Op.”).

searches of his communications—as agents do “whenever the FBI opens a new national security investigation or assessment[.]” PCLOB Report 59. Indeed, the FBI’s publicly available minimization procedures expressly permit and encourage such backdoor searches. *See* FBI Section 702 Minimization Procedures at 11 & n.3 (2015), <https://perma.cc/G3X4-FT92> (queries of Section 702 databases are “a routine and encouraged practice”).

Beyond its boilerplate notice of Section 702 surveillance, V1 at 552, the government refused to provide Mr. Muhtorov or his lawyers with virtually any information about its use of that surveillance in this case. The government has not told Mr. Muhtorov which of his communications it obtained under Section 702; whether they were phone calls, emails, Skype video calls, or web pages he visited; or how his communications were used in the government’s investigation. It has not provided Mr. Muhtorov with its surveillance applications, the supporting affidavits, or the FISC orders that granted those applications. It has not provided Mr. Muhtorov with the targeting and minimization procedures that applied at the time his communications were collected. Nor, finally, has it told Mr. Muhtorov what search terms or other methods agents used to locate his communications in the government’s Section 702 databases.¹²

¹² The government vaguely asserted below that “[t]his case does not involve upstream collection.” V3 at 600. That representation is inadequate. Mr. Muhtorov does not know whether PRISM or another type of Section 702 surveillance was

Without these basic facts, Mr. Muhtorov’s arguments are confined to the limited information available to him. The Court should ensure that defense counsel have the opportunity to address any issue, legal or factual, that may bear on the challenged surveillance. *See infra* Part II.

C. The search and seizure of Mr. Muhtorov’s communications violated the Fourth Amendment’s warrant requirement.

Under the Fourth Amendment, Americans have a protected privacy interest in the contents of their communications, including their telephone calls and emails. *See United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313 (1972); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The government therefore needs a warrant to search and seize these communications. Searches conducted without a warrant are “per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Katz v. United States*, 389 U.S. 347, 357 (1967).

Section 702 does not require the government to obtain a warrant based on probable cause prior to collecting the communications of Americans, nor does it impose any comparable requirement after the fact. The government’s collection, searching, and use of these communications is therefore presumptively

used, let alone how the searches were effectuated given modern technologies. Yet full and fair litigation of Fourth Amendment cases involving novel surveillance methods often turn on *how* a search is conducted.

unconstitutional. Moreover, no exception to the warrant requirement exists that could justify such a sweeping program of suspicionless searches.

1. Section 702 permits surveillance of Americans’ international communications in violation of the warrant requirement.

The Fourth Amendment’s warrant requirement carries with it three fundamental protections: (1) a search warrant must be issued by a neutral, disinterested magistrate; (2) the government must demonstrate probable cause to believe that the evidence sought will aid in a particular apprehension or conviction; and (3) the warrant must particularly describe the things to be seized and the places to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979).

Surveillance under Section 702 is conducted without any of the familiar safeguards that a warrant provides. It is therefore presumptively unconstitutional. *See Katz*, 389 U.S. at 357. Moreover, none of the warrant requirement’s “jealously and carefully drawn” exceptions apply to the surveillance at issue here. *Jones v. United States*, 357 U.S. 493, 499 (1958).¹³ Regardless of whether the warrant requirement applies to the communications of foreigners overseas, it unquestionably reaches the communications of U.S. persons on U.S. soil.

¹³ Indeed, the district court declined to identify any applicable exception to the warrant requirement, calling the issue “somewhat academic.” V3 at 139.

Accordingly, the government must, at a minimum, obtain a warrant when it deliberately seeks to use or search for the communications of Americans like Mr. Muhtorov. Especially in the context of electronic searches, courts have frequently required the government to obtain a warrant *after* its initial seizure or search. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2493 (2014) (requiring government to obtain a warrant before searching cell phone lawfully seized incident to arrest); *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (requiring government to obtain a warrant before conducting new search of lawfully seized computer hard-drive).

2. The government must obtain a warrant to search and use Americans’ communications regardless of whether it is “targeting” foreigners.

The government argued below that incidental collection of a U.S. person’s communications during surveillance targeting non-U.S. persons abroad does not implicate the warrant clause at all. V1 at 787-88. But the rule the government cites—sometimes called the “incidental overhear” rule—has no application here.

The government’s use of the term “incidental” conveys the impression that its collection of Americans’ communications under Section 702 is a de minimis or unintended byproduct, common to all forms of surveillance. In reality, however, the warrantless surveillance of Americans’ communications under Section 702 was

both the purpose and the direct result of the statute.¹⁴ Moreover, the *volume* of communications intercepted “incidentally” under Section 702 dwarfs that of communications intercepted incidentally under the original provisions of FISA or Title III.¹⁵

The government relied on the “incidental overhear” rule to argue that so long as it claims to be targeting foreigners, agents may read and listen in on the private communications of Americans without a warrant. V1 at 787. But the “incidental overhear” cases do not establish an exception to the warrant requirement. The formative cases establishing this rule apply it only when the government has *sought and obtained* a valid warrant. *See, e.g., United States v. Kahn*, 415 U.S. 143 (1974); *United States v. Donovan*, 429 U.S. 413, 418 (1977); *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985). Far from announcing an exception to the warrant requirement, these cases honor it. *See* Elizabeth

¹⁴ *See* PCLOB Report 82, 86-87 (“Such ‘incidental’ collection of communications is not accidental, nor is it inadvertent”).

¹⁵ *See, e.g.,* President’s Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 149 (2013), <https://perma.cc/9LYQ-DVJL> (“PRG Report”) (“incidental interception is significantly more likely to occur when the interception takes place under section 702 than in other circumstances”).

Goitein, *The Ninth Circuit's Constitutional Detour in Mohamud*, Just Security (Dec. 8, 2016), <https://goo.gl/G8wT3X>.¹⁶

Indeed, the government simply ignored the rationale for the incidental overhear rule: the commonsense principle that a single warrant protects the privacy interests of *both* parties to a communication. The warrant process is exacting by design. It requires courts to carefully circumscribe surveillance, confining it to conversations that are evidence of a particular crime and limiting the intrusion as to both the target and any person with whom the target communicates. Thus, when the government has established probable cause to seize certain communications—and has thereby satisfied the necessary Fourth Amendment threshold—its warrant satisfies the privacy interests of each party to the communications, including parties who are incidentally overheard. *See Figueroa*, 757 F.2d at 471; PCLOB Report 95. Because of this, the incidental overhear cases simply stand for the proposition that the government need not obtain *multiple* warrants to intercept protected communications. *See Kahn*, 415 U.S. at 153. By contrast, the “complete

¹⁶ The Ninth Circuit is the only court of appeals to have addressed the lawfulness of Section 702, *see United States v. Mohamud*, 843 F.3d 420, 439-41 (9th Cir. 2016), in a decision that makes the same errors as the government and has been sharply criticized. *See* Orin Kerr, *The Surprisingly Weak Reasoning of Mohamud*, Lawfare (Dec. 23, 2016), <https://bit.ly/2PfkPWx>.

absence of prior judicial authorization would make an [incidental] intercept unlawful.” *Donovan*, 429 U.S. at 436 n.24.

The surveillance in this case—like all Section 702 surveillance—did not involve a warrant. There was no showing of probable cause; there was no individualized judicial review; and there was no attempt at particularity. That the government’s “target” was not a U.S. person may be sufficient to allow the government to warrantlessly surveil *that* person. But the Fourth Amendment does not speak in terms of “targets.” What matters, for Fourth Amendment purposes, is that an American has a protected privacy interest in these communications. *See supra* Kerr, *The Surprisingly Weak Reasoning of Mohamud*. Even if the government claims to be targeting someone who lacks Fourth Amendment rights, it may not ignore the rights of a U.S. person like Mr. Muhtorov, who *is* entitled to that protection.

The district court dispensed with the warrant requirement almost in passing, pointing to the Supreme Court’s ruling in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). V3 at 138-139. But that case does not authorize the warrantless surveillance of Americans like Mr. Muhtorov on U.S. soil.

Verdugo-Urquidez involved a search of physical property located in Mexico and belonging to a Mexican national, in circumstances where no U.S. court had authority to issue a warrant. *See* 494 U.S. at 261-62, 274. *Verdugo-Urquidez* was

solely concerned with the warrant requirement's application *abroad*. The search was conducted on *foreign* soil; the privacy interests at stake were exclusively those of a *foreign* national; and the subject of the search was, until his arrest, located *abroad*.

The search of Mr. Muhtorov's communications has nothing in common with *Verdugo-Urquidez*.

First, the search here took place inside the United States—and, as the Supreme Court made clear, that fact matters immensely. *See id.* at 278 (Kennedy, J., concurring) (“If the search had occurred in a residence within the United States, I have little doubt that the full protections of the Fourth Amendment would apply.”); *id.* at 261-62, 264, 274-75.

Second, Mr. Muhtorov is a U.S. person, unlike the respondent in *Verdugo-Urquidez*. Thus, even if the government is correct that the Fourth Amendment does not protect foreigners abroad, Mr. Muhtorov's case does not involve such a claim. What matters here is that the government acquired a communication to which an American was a party—a communication to which the Fourth Amendment unquestionably applies. Nothing in *Verdugo-Urquidez* suggests that Americans forfeit their right to privacy whenever they communicate with individuals abroad.

Finally, longstanding historical practice confirms that *Verdugo-Urquidez* does not license the surveillance here. The government has never been able to

warrantlessly seize and search the private letters, phone calls, and emails of Americans on U.S. soil simply by pointing to a foreigner on the other end. *See, e.g., Ex parte Jackson*, 96 U.S. 727, 733 (1877); *United States v. Ramsey*, 431 U.S. 606, 623-24 (1977) (citing regulations requiring a warrant to read the contents of international letters on U.S. soil); 18 U.S.C. § 2518 (warrant required for interception of phone calls and emails on U.S. soil in criminal investigations). The government’s sweeping arguments would upend this bedrock protection, in routine criminal investigations and national-security cases alike.

3. If there is a foreign-intelligence exception to the warrant requirement, it is not broad enough to render the surveillance of Mr. Muhtorov constitutional.

The government also argued below that the warrant requirement does not apply here because Section 702 surveillance serves a foreign-intelligence purpose and therefore falls within the “special needs” doctrine. V1 at 791. This is incorrect. Courts recognize an exception to the warrant requirement only “in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.” *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

The mere fact that the government conducts this surveillance to acquire foreign-intelligence information does not render the warrant and probable-cause requirements unworkable. In *Keith*, the Supreme Court expressly rejected the

government’s argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316-21. That logic applies with equal force to surveillance directed at targets with a foreign nexus—at least when that surveillance sweeps up Americans’ communications (as Section 702 surveillance does), and is conducted inside the United States (as Section 702 surveillance is).

The Supreme Court has never recognized a foreign-intelligence exception to the warrant requirement, nor has this Court. But even if such an exception exists, it is not broad enough to render Section 702 surveillance constitutional. Courts have approved narrow modifications to the probable-cause requirement when considering individualized surveillance under FISA, but only where the surveillance in question was (1) directed at foreign powers or their agents; and (2) predicated on an individualized finding of suspicion. *See, e.g., United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir. 1984); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002).

Section 702 contains no such limitations. The surveillance is not confined to “foreign powers or agents of foreign powers reasonably believed to be located outside the United States”—a limitation the Foreign Intelligence Surveillance Court of Review (“FISCR”) deemed critical in analyzing similar surveillance. *In re Directives*, 551 F.3d 1004, 1012-16 (FISCR 2008). Instead, under Section 702, the

government may target *any* non-citizen outside the United States to acquire “foreign intelligence information,” broadly defined. Moreover, where prior cases required a probable-cause determination by the President or Attorney General, *see, e.g., id.*, under Section 702, targeting decisions have been handed off to an untold number of government analysts. As the Privacy and Civil Liberties Oversight Board observed, no court has ever recognized a foreign-intelligence exception sweeping enough to render constitutional the surveillance at issue here. *See* PCLOB Report 90 n.411.

While foreign-intelligence gathering is unquestionably a government interest of the highest order, it does not exempt surveillance of Americans from the warrant requirement.

D. The surveillance of Mr. Muhtorov violated the Fourth Amendment’s reasonableness requirement.

Even if the government is permitted to surveil foreigners without first obtaining a warrant, it is not entitled to completely bypass the Fourth Amendment rights of Americans like Mr. Muhtorov. Rather, the government’s reasoning would justify, at most, the warrantless acquisition of foreign-to-foreign communications, in which it says no Fourth Amendment interests are implicated. But instead the government seeks a windfall: the ability to retain, use, and deliberately query its massive Section 702 databases for the emails of known Americans, without ever satisfying bedrock Fourth Amendment requirements. Regardless of whether the

warrant requirement applies, “the ultimate touchstone of the Fourth Amendment is reasonableness,” *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006), and the government’s purposeful exploitation of Americans’ communications in this manner is unreasonable.

To the extent the government claims it is unable to avoid seizing Americans’ communications in the first place, reasonableness requires that it provide comparable Fourth Amendment protection to Americans *after* its initial seizure. At a minimum, agents must obtain individualized judicial approval at the point when they seek to query or use an American’s communications. Because Section 702 has no such post-seizure limitations, the surveillance of Mr. Muhtorov was unreasonable.

1. Section 702 surveillance lacks the core safeguards that courts require when assessing the reasonableness of electronic surveillance.

Under the Fourth Amendment, reasonableness is determined by examining the “totality of the circumstances” to “assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *Samson v. California*, 547 U.S. 843, 848 (2006). In the context of electronic surveillance, reasonableness requires that government eavesdropping be “precise and discriminate” and “carefully circumscribed so as to

prevent unauthorized invasions” of privacy. *Berger v. New York*, 388 U.S. 41, 58 (1967); see *United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973).

Courts assessing the lawfulness of electronic surveillance have looked to FISA and Title III as measures of reasonableness. See *United States v. Mesa-Rincon*, 911 F.2d 1433, 1437-39 & n.5 (10th Cir. 1990) (evaluating reasonableness of video surveillance). While the limitations on foreign-intelligence surveillance may differ in some respects from those applicable to law-enforcement surveillance, “the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns.” *In re Sealed Case*, 310 F.3d at 737.

Section 702 abandons three core safeguards—individualized judicial review, a finding of probable cause, and particularity—that courts, including this one, have relied on to uphold the constitutionality of FISA, Title III, and other novel forms of surveillance. *Duggan*, 743 F.2d at 73-74 (FISA); *United States v. Tortorello*, 480 F.2d 764, 772-73 (2d Cir. 1973) (Title III); *Mesa-Rincon*, 911 F.2d at 1437-39.

First, Section 702 fails to interpose “the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police.” *Katz*, 389 U.S. at 357. The Fourth Amendment reflects a judgment that “[t]he right of privacy [is] too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals.” *McDonald v. United States*, 335 U.S. 451, 455-56 (1948). But under Section 702, the FISC’s role is limited to reviewing the government’s

targeting and minimization procedures. Every decision concerning specific surveillance targets is left to the discretion of executive-branch employees, even as these decisions affect countless Americans. *See Riley*, 134 S. Ct. at 2491 (“[T]he Founders did not fight a revolution to gain the right to government agency protocols.”).

Second, Section 702 fails to condition surveillance on the existence of probable cause of any kind. It permits the government to conduct surveillance without demonstrating to a court that the people it seeks to surveil are foreign agents, engaged in criminal activity, or connected—even remotely—with terrorism. 50 U.S.C. § 1881a(a). It permits the government to conduct surveillance without even an executive-branch determination that its targets belong to any of these categories.

Third, surveillance under Section 702 is not particularized. Instead, it permits the government to collect—wholesale and on an ongoing basis—all communications to and from more than 160,000 targets. The requirement of particularity “is especially great in the case of eavesdropping,” which inevitably results in the interception of unrelated, intimate conversations. *Berger*, 388 U.S. at 56. Unlike Title III and FISA, however, Section 702 does not require the government to identify to any court the telephone lines, email addresses, or places

at which its surveillance will be directed, or “the particular conversations to be seized.” *Donovan*, 429 U.S. at 427 n.15.

The consequence of Section 702’s failure to include these limitations is that government agents may target a vast number of foreigners for surveillance—and may thereby collect the emails and phone calls of all Americans communicating with those foreigners.

2. The Section 702 procedures allow and encourage the warrantless exploitation of Americans’ communications, including through backdoor searches.

The constitutionality of electronic surveillance regimes depends not just on limitations on initial collection but also on the restrictions on later retention and use. Because Section 702 is extremely permissive at the outset—allowing the broad, continuous collection of billions of communications—strong post-seizure restrictions on the use of this information are critical to the Fourth Amendment analysis. In assessing such restrictions, the government’s justification for its initial search matters. Where, as here, the government justifies warrantless surveillance by asserting that its foreign targets lack Fourth Amendment rights, its subsequent use and querying of *Americans’* communications without any individualized judicial approval is unreasonable. *See In re Directives*, 551 F.3d at 1015 (finding warrantless surveillance of foreigners reasonable only after the government represented that it was not amassing databases of Americans’ incidentally collected

communications); *see generally Terry v. Ohio*, 392 U.S. 1, 19 (1968) (“The scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible.”).

Because of the “inherent dangers” and overbreadth of electronic searches, courts have long looked to post-seizure limitations when analyzing the reasonableness of surveillance. *Berger*, 388 U.S. at 60. For example, in *Berger*, the Supreme Court faulted New York’s eavesdropping statute in part because it did not limit the surveillance to particular conversations, but instead permitted the retention and use of “any and all conversations” of the state’s targets; it did not meaningfully constrain the duration of surveillance; and it did not provide for after-the-fact notice to those monitored. *See id.* at 58-60. Drawing heavily on *Berger*, this Court upheld the constitutionality of video surveillance in *Mesa-Rincon*—but only after insisting on “precise” minimization rules that prevented the government from continuously and indiscriminately recording private activities. 911 F.2d at 1439-1441; *see Tortorello*, 480 F.2d at 772-73, 783-84 (Title III). Likewise, courts considering the reasonableness of foreign-intelligence surveillance have relied on FISA’s minimization procedures, which regulate how the government may retain, use, and disseminate the information it obtains. *See In re Sealed Case*, 310 F.3d at 740. These cases belie the government’s claim that so long as its targeting of foreigners was “lawful” at the outset, the Fourth

Amendment has nothing to say about its subsequent querying or use of Americans' communications. V1 at 818.

The government's insistence that it can freely exploit Americans' emails and phone calls without further judicial approval is at odds, too, with another line of Supreme Court cases. Because the Fourth Amendment carries a continuing requirement of reasonableness, the government's duties often change as its search or seizure becomes more intrusive. *See Rodriguez v. United States*, 135 S. Ct. 1609, 1614-15 (2015) (traffic stop that was lawful when initiated violated Fourth Amendment when officer's investigation expanded beyond original justification); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (reasonableness of warrantless drug tests depended on protections against later dissemination of the results); *United States v. Place*, 462 U.S. 696, 709-10 (1983) (a seizure lawful at its inception can nevertheless violate the Fourth Amendment based on agents' subsequent conduct). Even if a warrantless search or seizure is lawful when initiated, reasonableness limits how far agents may intrude on protected interests before they must obtain judicial approval.

Strong post-seizure restrictions are especially critical under Section 702 given the breadth of the collection and the absence of traditional Fourth Amendment safeguards at the outset. Here, they would also answer one of the government's principal objections: that it would be impractical to obtain a warrant

beforehand, because it cannot know whether surveillance directed at a given foreigner will sweep up protected communications involving Americans. V1 at 789. But that fact—even if true in some instances—does not excuse the government from obtaining individualized judicial approval when it later seeks to use communications that it knows *are* protected. At the very least, reasonableness requires the provision of safeguards for Americans after the fact.¹⁷

Indeed, both Congress and courts—including this Court—have often dealt with similar overbreadth or overseizure problems, especially when confronted with broad seizures of digital information. In response, they have imposed rules to ensure that the government’s *use* of seized data does not exceed its Fourth Amendment authority. These rules routinely require the government either to refrain from using information beyond the scope of its legal authority or to secure additional court authorization after the fact.

For instance, in the case of traditional FISA surveillance, Congress imposed strict minimization rules to ensure that *warrantless* surveillance directed exclusively at foreign powers—for example, surveillance of foreign embassies in the U.S.—does not intrude upon the rights of Americans swept up in that

¹⁷ See Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, Lawfare (Oct. 19, 2017), <https://goo.gl/RHqdND>; Geoffrey Stone & Michael Morell, *The One Change We Need to Surveillance Law*, Wash. Post, Oct. 9, 2017, <http://wapo.st/2hZ1xJx>.

surveillance. *See* 50 U.S.C. §§ 1801(h)(4), 1802(a)(1). If the government learns after the fact that it has collected an American's communications without a warrant, it is required to destroy the protected communications within 72 hours or to obtain an individualized FISC order to retain them. *Id.* § 1801(h)(4). Because this surveillance is warrantless and targeted at foreign powers, it is closely analogous to that conducted under Section 702.

When the FISC examined warrantless surveillance conducted under Section 702's predecessor statute, the Protect America Act, it held the surveillance reasonable only after finding that the government was *not* amassing a searchable database of Americans' incidentally collected communications. *See In re Directives*, 551 F.3d at 1015; *see also* [Redacted], 2011 WL 10945618, at *23 & n.60 (approving procedures that prohibited NSA from querying Americans' communications in its Upstream databases).

In the case of computer hard-drive searches, where data is often intermingled, this Court has also recognized the importance of post-seizure restrictions. Even when the government lawfully seizes the *full* contents of a device pursuant to a warrant, it may only search for the particular information authorized by the original probable-cause warrant—at least not without obtaining further court authorization. *See United States v. Loera*, 923 F.3d 907, 922-23 (10th Cir. 2019); *Sedaghaty*, 728 F.3d at 913.

In each of these instances, either courts or Congress have imposed workable solutions to ensure that the government’s electronic searches are properly confined. Similarly here, the mere fact that the government is “targeting” foreigners when it acquires Americans’ protected communications is not a valid reason to jettison the safeguards that a warrant would otherwise afford.

While post-seizure restrictions could adequately protect the rights of Americans under Section 702, the existing procedures do the opposite. They allow the government to collect Americans’ communications on U.S. soil without a warrant. They allow the government to retain those communications for five years by default—and to pool them in massive centralized databases. And they allow agents to conduct queries that deliberately target Americans’ communications after they are collected, including for use in criminal investigations. PCLOB Report 55-60. In short, the procedures authorize the very type of intrusion that the Fourth Amendment was designed to guard against.¹⁸

¹⁸ In analyzing reasonableness, the district court wrongly held that Mr. Muhtorov’s privacy interest was “somewhat diminished” by the fact that his communications were “transmitted to a third party over the internet.” V3 at 142. It is virtually axiomatic that communications include more than one party, but that has not diminished the constitutional protection they receive. *See, e.g., Katz*, 389 U.S. at 351-52 (telephone conversations). Indeed, as the Supreme Court recently observed, Americans’ digital papers are entitled to “full Fourth Amendment protection,” even when held by third-party companies. *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018) (citing *Warshak*, 631 F.3d at 283-88).

3. The government has reasonable alternatives that would allow it to collect foreign intelligence while protecting Americans' private communications.

The government has reasonable alternatives at its disposal. Compliance with the Fourth Amendment requires at least one of two things: that the government avoid warrantless *acquisition* of Americans' communications, if it is reasonably possible to do so; or that it obtain judicial approval to *search for* or *use* Americans' communications when it has collected them warrantlessly. There is no practical reason why these limitations—which have the effect of requiring safeguards only for Americans' communications—could not be imposed here.

Indeed, a number of proposals would permit the government to continue collecting foreign-to-foreign communications while providing additional protections for communications involving Americans. Years before the government's backdoor searches came to light, the Senate debated an amendment that would have prohibited the government from (1) acquiring a communication without a warrant if it knew “before or at the time of acquisition that the communication [was] to or from a person reasonably believed to be located in the United States,” and (2) accessing Americans' communications collected under Section 702 without a warrant. *See* S.A. 3979, 110th Cong. (2008), 154 Cong. Rec. S607-08 (daily ed. Feb. 4, 2008). More recently, the President's Review Group concluded that a warrant requirement should be imposed, and the House of

Representatives passed a bill that would prohibit the retention and use of Americans' communications. *See* PRG Report 28-29; H.R. 4870, 113th Cong. § 8127 (2014).

The government argued below that complying with the warrant requirement would be unworkable because “imposition of a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection.” V1 at 789. Not so. The Fourth Amendment does not require the government to obtain prior judicial authorization for surveillance of foreign targets merely because those foreign targets might communicate with U.S. persons. Rather, the Fourth Amendment requires the government to take reasonable steps to avoid the warrantless interception, retention, and use of Americans' communications. Section 702 surveillance lacks even basic protections that would prevent these warrantless intrusions. As a consequence, it is unreasonable.

E. The warrantless surveillance of Mr. Muhtorov violated Article III of the Constitution.

The Section 702 surveillance of Mr. Muhtorov violated Article III because the statute authorizes the FISC to issue mass surveillance orders in the absence of any case or controversy, and it requires the court to review the legality and constitutionality of the government's procedures in the abstract. The district court cursorily rejected this argument, but it provides an independent ground for

invalidating the surveillance of Mr. Muhtorov. V3 at 137 (“Whether [the FISC’s] role offends Article III sufficiently to invalidate § 702 as a tool for gathering foreign intelligence information is one I leave to a higher court.”).

The Constitution “extend[s]” the judicial power of the United States to only “cases” and “controversies.” U.S. Const. art. III, § 2. That requirement is a condition precedent to the exercise of judicial authority, “restrict[ing]” federal courts to the “resolution of concrete disputes between the parties before them.” *Sec’y of State of Md. v. Joseph H. Munson Co.*, 467 U.S. 947, 976 (1984); *accord Massachusetts v. EPA*, 549 U.S. 497, 516 (2007). In other words, courts may pass only upon particularized issues capable of judicial resolution—“flesh-and-blood legal problems with data relevant and adequate to an informed judgment.” *New York v. Ferber*, 458 U.S. 747, 768 (1982). Conversely, courts are without the power to issue “abstract declaration[s] of the law,” *In re Summers*, 325 U.S. 561, 566-67 (1945), or adjudicate legal questions based “upon a hypothetical state of facts,” *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 241 (1937); *see also Flast v. Cohen*, 392 U.S. 83, 96-97 (1968).

Section 702 assigns to an Article III court a role that is fundamentally incompatible with the case-or-controversy requirement. Under Section 702, the government asks the FISC to issue mass surveillance orders that result in the acquisition of Americans’ communications without any individualized review or

approval of the government’s monitoring activity. The FISC’s role is limited to evaluating in a vacuum whether the government’s proposed targeting and minimization procedures comply with the statute and the Constitution, without any concrete factual context relating to particular targets. Article III “admonishes federal courts . . . to abstain from entangling themselves in abstract disagreements,” *Keyes v. Sch. Dist. No. 1*, 119 F.3d 1437, 1443 (10th Cir. 1997) (quotation marks omitted), but engagement with abstraction is exactly what Section 702 demands. And while Article III requires “application of principles of law or equity to facts,” *Vermont v. New York*, 417 U.S. 270, 277 (1974), Section 702 calls for an abstract assessment of the general rules that will govern a surveillance program to be implemented entirely by the executive branch.

It is instructive that, in rejecting Article III challenges to the traditional FISA process, district courts have pointed to the fact that the traditional FISA process is a particularized one—that it involves the court’s consideration of concrete facts about the specific person to be monitored, the facilities to be targeted, and the purpose of the surveillance. *See, e.g., United States v. Megahey*, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982) (“Applications for electronic surveillance submitted to FISC pursuant to FISA involve concrete questions respecting the application of the Act and are in a form such that a judge is capable of acting on them.”).

The Office of the Legal Counsel (“OLC”) relied on the same reasoning in defending the constitutionality of FISA in the debate preceding the statute’s enactment. Key to the OLC’s analysis was the fact that the FISC would be able to “apply standards of law to the facts of a particular case” in the form of probable-cause determinations akin to those “made in other warrant proceedings.” *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 26, 28 (1978) (statement of John Harmon, Asst. Att’y Gen., OLC).

Thus, as both the judicial and executive branches have recognized, a traditional FISA order presents the court with a concrete question about a particular proposed interception. *See also* Elizabeth Goitein & Faiza Patel, *What Went Wrong with the FISA Court*, Brennan Center for Justice 7 (Mar. 2015), <https://bit.ly/2KKhxtE>. By contrast, a mass surveillance order under Section 702 demands only a broad assessment of whether the government’s minimization and targeting procedures are reasonable—a question asked and answered at the highest level of generality without reference to particular persons or facilities. *Id.* at 29-34. That question is simply not a case or controversy appropriate for judicial resolution under Article III.

F. FISA mandates suppression when a court concludes that surveillance was unlawful.

Not only is Mr. Muhtorov entitled to suppression under the Fourth Amendment, but FISA itself provides a mandatory statutory remedy. If the Court “determines that the surveillance was not lawfully authorized or conducted, it *shall* . . . suppress the evidence which was unlawfully obtained or derived” from such surveillance. 50 U.S.C. § 1806(g) (emphasis added). “This ground for suppression plainly includes constitutional challenges to FISA itself.” David S. Kris & J. Douglas Wilson, *2 National Security Investigations & Prosecutions* § 32:3 (2d ed. 2012). Thus, if the Court finds that the government’s surveillance of Mr. Muhtorov’s communications was unlawful in this case, he is entitled to suppression under Section 1806(g).

II. Given the novelty and complexity of the challenged surveillance, disclosure of the Section 702 and FISA materials was required.

In moving to suppress the fruits of Section 702 and traditional FISA surveillance, Mr. Muhtorov faced a substantial obstacle: the government’s refusal to disclose *any* of the underlying applications, orders, or similar materials related to this surveillance. Deprived of this information, Mr. Muhtorov was unable to make the full range of legal, factual, and technological arguments that a court must analyze in reviewing the complex surveillance used here. In short, the district court

lacked the benefit of informed adversarial argument on questions bearing directly on the legality of this surveillance.

Both FISA and due process require the disclosure of the materials sought by Mr. Muhtorov, and the district court erred in holding otherwise. FISA itself requires the court to order disclosure of materials to Mr. Muhtorov's counsel, because disclosure was "necessary" for an "accurate determination of the legality" of the surveillance. 50 U.S.C. §§ 1806(f), 1825(g), 1881e. Congress has made clear that disclosure is "necessary" in cases like this one, which involves novel and complex legal and factual issues. And if there were any uncertainty as to whether FISA requires disclosure, the statute must be construed consistent with the Fourth and Fifth Amendments, which compel disclosure in Mr. Muhtorov's case.

Separately, the government's claim of secrecy over *all* of the Section 702 and FISA materials at issue is not credible. The government has made numerous public disclosures of Section 702 and FISA materials, yet it refused to give Mr. Muhtorov access to comparable information. Due process prohibits the government from relying on pro forma claims of secrecy to deprive criminal defendants of materials helpful to their defense.

A. Preservation and standard of review.

Mr. Muhtorov's challenge to the government's withholding of Section 702 and FISA materials was raised and ruled on below. V1 at 373, 380 (FISA motion);

V1 at 666, 712 (Section 702 motion); V1 at 479, 480 (FISA order); V3 at 115, 148-49 (Section 702 order). This Court reviews de novo the district court's legal conclusion that neither FISA nor due process require disclosure in novel or complex cases like this one. *See United States v. Porter*, 745 F.3d 1035, 1040 (10th Cir. 2014); 50 U.S.C. §§ 1806(f), 1825(g); V3 at 116, 128-29 (recognizing novelty of surveillance); V11 at 259 (recognizing complexity).¹⁹

B. Background and statutory framework.

Unlike defendants who challenge searches in other criminal cases, a defendant who seeks to challenge FISA surveillance has virtually no information. Although the government's evidence in this case appears to have been the product of near-total surveillance of Mr. Muhtorov and his family, he has never seen the underlying applications or orders that supplied the basis for that surveillance. Even when Mr. Muhtorov became the first person ever to receive notice of Section 702 surveillance, the government provided only a boilerplate notification, bereft of detail. V1 at 220, 552.

Under FISA, a defendant may move for disclosure of applications, orders, and other materials related to the surveillance. 50 U.S.C. §§ 1806(e), 1825(f).

¹⁹ In addition to his Section 702 challenge, Mr. Muhtorov moved to suppress the fruit of the traditional FISA surveillance in the district court. V1 at 373. He also seeks to renew that motion to suppress with the benefit of the critical disclosures sought here.

Given the variety of surveillance techniques potentially at issue, Mr. Muhtorov sought disclosure of basic information about the FISA and Section 702 surveillance of his communications, so that he could craft informed motions to suppress. V1 at 380, 712.

When a defendant seeks disclosure, the Attorney General may file an affidavit asserting that disclosure would harm the national security of the United States. If the Attorney General files such an affidavit—as the Attorney General has done in every case since 1978 in which a defendant sought to challenge FISA surveillance, *see* V1 at 848—the district court must review the surveillance materials *ex parte* “as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” 50 U.S.C. §§ 1806(f), 1825(g).

The statute recognizes, however, that in some cases the district court’s *ex parte* review will not be sufficient, and that an adversarial process will be necessary. Thus, the statute provides that, following the court’s initial review, the court may disclose FISA materials to the defendant under appropriate security procedures “where such disclosure is necessary to make an accurate determination of the legality” of the surveillance or searches. *Id.*

Here, the district court denied Mr. Muhtorov’s motions for disclosure. V1 at 480; V3 at 148-49. For the reasons below, that decision was erroneous.

C. Disclosure of the Section 702 and FISA materials was “necessary” for an accurate determination of the legality of the surveillance.

In denying Mr. Muhtorov’s motions for disclosure, the district court construed Sections 1806(f) and 1825(g) far too narrowly. Mr. Muhtorov’s Section 702 and FISA challenges present legal issues of first impression in this circuit and factual issues of significant complexity. Given the complexity and novelty of the issues here, as well as the volume of materials, disclosure of Section 702 and FISA materials to Mr. Muhtorov’s defense team was “necessary” for an “accurate determination of the legality” of the surveillance. 50 U.S.C. §§ 1806(f), 1825(g).

1. FISA’s text, structure, and legislative history confirm that disclosure is “necessary” in cases involving complex questions.

FISA’s text, structure, and legislative history make plain that disclosure is necessary in complex cases such as this one.

The text and structure of Sections 1806 and 1825 are clear that disclosure is appropriate in certain circumstances. The statute allows defendants to move for disclosure of Section 702 and FISA materials, and it empowers district courts to order the disclosure of Section 702 and FISA materials, notwithstanding the government’s secrecy claims.

As the statute’s legislative history confirms, Congress anticipated that FISA materials would be disclosed in cases involving complex issues of fact or law. In enacting FISA, Congress sought to “strik[e] a reasonable balance” between

“mandatory disclosure” and “an entirely in camera proceeding which might adversely affect the defendant’s ability to defend himself.” *E.g.*, S. Rep. No. 701, 95th Cong., 2d Sess. at 64, *reprinted in* 1978 U.S.C.C.A.N. 4033. The congressional reports also describe factors that Congress expected courts to consider when assessing whether disclosure is “necessary”: the “complex[ity]” of the legal questions at issue; “indications of possible misrepresentations of fact”; and the “volume, scope, and complexity” of the surveillance materials. *Id.* Courts have since explained that disclosure is “necessary” when these factors are present. *See, e.g., United States v. Belfield*, 692 F.2d 141, 147-48 (D.C. Cir. 1982).

Here, these factors require disclosure.

2. Mr. Muhtorov’s challenge involves significant legal, factual, and technological complexity.

If disclosure is “necessary” for an “accurate” determination of legality in any case, it is in this one. To assess the lawfulness of the Section 702 and FISA surveillance of Mr. Muhtorov, the district court had to evaluate an array of complex legal, factual, and technological issues. Based on the unclassified record, it appears that the district court failed to engage with many of these issues. And as recent cases have shown, reliance on one-sided submissions from the government in complex surveillance litigation carries an unacceptably high risk of error. *See ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015); [*Redacted*], 2011 WL 10945618, at *9.

With respect to Section 702 surveillance, the court had to address the following questions, among others, without the benefit of informed adversarial argument:

First, the court had to evaluate whether the mass surveillance order authorizing the Section 702 surveillance of Mr. Muhtorov complied with the Fourth Amendment and the statute. Because this analysis must take into account *how* the government obtains communications, it involves significant technical complexity. Under Section 702, the government implements vastly different forms of surveillance, with distinct technological features that raise distinct legal questions. *See, e.g.*, PCLOB Report 33-41. Yet the government never disclosed which specific form(s) of Section 702 surveillance it used to obtain Mr. Muhtorov's communications.

Second, the court had to assess whether the government's Section 702 application(s) to the FISC contained material omissions or misrepresentations. *See Franks v. Delaware*, 438 U.S. 154, 155 (1978). As discussed below, the government has a long track record of material misrepresentations and omissions in the FISC. These misrepresentations may not be evident from the face of the applications, but can often be identified only by probing how Section 702 is applied to various types of internet communications. *See [Redacted]*, 2011 WL 10945618, at *9. Because the court denied Mr. Muhtorov access to the

government's applications and the FISC's orders, Mr. Muhtorov was unable to effectively identify misrepresentations related to the surveillance of his communications.

Third, the court had to determine whether the specific Section 702 targeting and minimization procedures that applied to Mr. Muhtorov's communications complied with the Fourth Amendment and FISA—and whether the government adhered to those procedures here. Yet the court denied Mr. Muhtorov access to the procedures, as well as information about the nature and number of the intercepted communications, severely limiting his ability to challenge the adequacy of the procedures and their application.

Fourth, the court had to determine whether the government's backdoor searches of Mr. Muhtorov's communications were constitutional. But the court denied Mr. Muhtorov access to information about how his communications were first identified, as well as information about the queries that agents used to locate and review his communications in the government's databases. While Mr. Muhtorov has challenged the government's use of backdoor searches, *see supra* Part I, he lacks specific information about how those searches were conducted and used here.

With respect to the traditional FISA surveillance directed at Mr. Muhtorov, the court had to consider similarly difficult questions:

First, the court had to evaluate whether the various FISA techniques complied with the Fourth Amendment and the statute. Because this analysis must take into account *how* the government obtains communications, it involves significant technical complexity. The government appears to have collected a vast amount of private information about Mr. Muhtorov (as well as his wife and children), using a wide array of highly intrusive techniques. *See supra* Statement of the Case. Yet the district court does not appear to have considered the Fourth Amendment issues presented by these techniques, especially in light of the relaxed showing required to obtain a FISA order (as compared to a warrant). *See* 50 U.S.C. §§ 1805, 1824; V1 at 373 (motion to suppress). Nor does the court appear to have considered what type of minimization rules are legally required when new technologies permit the government to collect far more private information than was previously possible, and to retain it in searchable FBI databases for years. V1 at 386, 397; *cf. Riley*, 134 S. Ct. at 2484-85, 2488-91. Instead, the court denied Mr. Muhtorov access to the FISA orders and minimization procedures.

Second, the court had to assess whether the government’s applications to the FISC contained material omissions or misrepresentations of fact—especially as to its claim that Mr. Muhtorov was a “foreign agent.” *See Franks*, 438 U.S. at 155. Based on the limited information available, Mr. Muhtorov identified several potential defects in the government’s FISA applications. V1 at 373, 382-94.

However, without disclosure, Mr. Muhtorov had no practical avenue to effectively challenge those applications. *See infra* Part II.D.

Finally, the court had to determine whether the FISA applications were tainted by other unconstitutional searches. *See Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963). This question is enormously complex. While some of the information in the government’s FISA application was obtained pursuant to Section 702, *see* V3 at 148, other information was likely obtained using other novel or illegal techniques, such as the warrantless collection of cell-site location data or the bulk collection of call records. *See infra* Part III.C. Without access to the FISA applications, however, Mr. Muhtorov could not raise those arguments.

If there were any doubt about the number and difficulty of the issues before the district court, declassified FISC opinions underscore the complexity of the government’s Section 702 and FISA surveillance—and the inherent limitations of *ex parte* proceedings in cases involving novel surveillance techniques. These opinions show that the government has made a series of incomplete or inaccurate representations in its surveillance applications, and that it has repeatedly failed to comply with restrictions imposed by the FISC. *Cf. Belfield*, 692 F.2d at 147 (disclosure is “necessary” where “the question of legality may be complicated by . . . indications of possible misrepresentations of fact”).

For example, while the investigation of Mr. Muhtorov was ongoing, the FISC held that Section 702 Upstream collection violated the Fourth Amendment—based on its discovery that the surveillance was significantly broader than the government had described for years. *See [Redacted]*, 2011 WL 10945618, at *9 (explaining that the “volume and nature of the information” the government had been collecting was “fundamentally different from what the Court had been led to believe”).

More recently, the FISC identified significant problems with the government’s backdoor searches of Section 702 data, as well as an array of other violations. *See* April 26, 2017 FISC Op. at 19-23, 68-95. After belatedly disclosing the backdoor-search problem, the NSA struggled for months to “ascertain the scope and causes” of its compliance problems, attributing its failure to “the complexity of the issues involved.” *Id.* at 5. This complexity was coupled with, in the FISC’s words, “an institutional ‘lack of candor’ on NSA’s part.” *Id.* at 19, 67-68 & n.57.²⁰

²⁰ The government has submitted misleading information to the FISC on a number of other occasions. *See* April 26, 2017 FISC Op. at 30 n.14 (noting other “substantial misrepresentation[s]” regarding “major collection programs”); *In re All Matters Submitted to the FISC*, 218 F. Supp. 2d 611, 620-21 (FISC 2002) (explaining “errors related to misstatements and omissions of material facts” in FISA applications), *abrogated on other grounds, In re Sealed Case*, 310 F.3d 717.

In short, Section 702 and FISA surveillance are so complex that the government has often failed to describe the surveillance accurately and has repeatedly violated its own procedures. This complexity only heightens the need for disclosure to defense counsel, as Congress recognized in FISA.

Moreover, the questions raised by the surveillance in this case were indisputably novel ones. Mr. Muhtorov's Section 702 and FISA challenges present legal issues of first impression in this circuit. When Mr. Muhtorov sought disclosure of Section 702 materials, no federal court had addressed the constitutionality of this surveillance. Even today, only one circuit court has analyzed the issue, in a decision that has been sharply questioned.²¹ While other courts have addressed traditional FISA surveillance, no court appears to have analyzed how the Fourth Amendment applies to the panoply of new, intrusive technologies directed at FISA targets like Mr. Muhtorov (and his family), including whether far more robust minimization rules are necessary to protect private, innocent communications in the face of such pervasive surveillance. *Cf. Riley*, 134 S. Ct. at 2488-91.

²¹ See Kerr, *The Surprisingly Weak Reasoning of Mohamud*, *supra*. A challenge to Section 702 surveillance is also pending before the Second Circuit. See *United States v. Hasbajrami*, No. 17-2669 (2d Cir.).

In light of the novelty and complexity of the techniques used in this case, disclosure of the Section 702 and FISA surveillance was “necessary” for the district court to make an accurate determination of its legality.

D. FISA must be construed to require disclosure consistent with the Fourth and Fifth Amendments.

Together, the Fourth and Fifth Amendments entitle defendants to a meaningful opportunity to seek suppression of evidence obtained illegally, and FISA’s disclosure provisions must be construed in light of this constitutional right. In Mr. Muhtorov’s case, the principle of constitutional avoidance requires that Sections 1806 and 1825 be read to require disclosure of Section 702 and FISA materials. *See Hooper v. California*, 155 U.S. 648, 657 (1895) (“[E]very reasonable construction must be resorted to in order to save a statute from unconstitutionality.”).

Under the Fifth Amendment’s Due Process Clause, defendants must have a meaningful opportunity to pursue suppression, which is the primary means of enforcing the Fourth Amendment’s guarantees. *See Wong Sun*, 371 U.S. at 487-88. Because Fifth Amendment due process protections apply in the pre-trial suppression context, circuit courts have held that the government must disclose information to a defendant that could affect the outcome of a suppression hearing. *See, e.g., United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) (“The suppression of material evidence helpful to the accused, whether at trial or on a

motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.”); *Smith v. Black*, 904 F.2d 950, 965-66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992) (due process mandates the disclosure of information in the government’s possession if nondisclosure would “affect[] the outcome of [a] suppression hearing”). In other words, due process entitles defendants—at a minimum—to information that is relevant and helpful to their arguments that evidence was obtained illegally and should be suppressed. *See Roviario v. United States*, 353 U.S. 53, 60 (1957).

Sections 1806 and 1825 must be construed against this constitutional backdrop. In particular, they must be construed to require disclosure of Section 702 and FISA materials in at least those cases where, as here, the surveillance raises unusually complex questions of fact and law. In these cases, disclosure under appropriate security measures is “necessary” for “an accurate determination of the legality” of the surveillance, 50 U.S.C. §§ 1806(f), 1825(g), and it is also necessary as a matter of constitutional right.

Adversarial process is almost always preferable, but it is especially necessary where factual or legal issues are unusually complex. As the Supreme Court has explained:

[T]he need for adversary inquiry is increased by the complexity of the issues presented for adjudication. . . . 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 which the Fourth Amendment exclusionary rule demands.

Alderman v. United States, 394 U.S. 165, 182, 184 (1969).

A traditional due process analysis also underscores that adversarial litigation is necessary at least where factual or legal issues are, as here, particularly novel or complex. Applying the familiar three-factor test in *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976), each factor weighs in favor of requiring disclosure. First, Mr. Muhtorov has a substantial interest in an accurate determination of whether the government's surveillance violated his rights. Second, where the factual and legal issues are particularly complex, a district court's in camera and ex parte review of the materials carries an unacceptably high risk of error. Finally, as discussed below, the government's boilerplate claims to secrecy in this context are profoundly undermined by its own public disclosures. Insofar as the government does have a legitimate interest in maintaining the secrecy of particular materials, that interest can be accommodated through "appropriate security procedures and protective orders." 50 U.S.C. §§ 1806(f), 1825(g).

Finally, not only was the district court's interpretation of FISA at odds with Mr. Muhtorov's constitutional right to a meaningful opportunity to seek suppression, but it was also in conflict with *Franks*, 438 U.S. 154. There, the

Supreme Court held that criminal defendants are entitled to an evidentiary hearing upon a “substantial preliminary showing” that a warrant affidavit includes a knowing or reckless false statement. *Id.* at 155-56. But as a practical matter, defendants like Mr. Muhtorov will virtually never be able to make the “substantial preliminary showing” required by *Franks*, because they cannot identify falsehoods or omissions in FISA affidavits they have not seen. *See United States v. Daoud*, 755 F.3d 479, 485-86 (7th Cir. 2014) (Rovner, J., concurring) (“[T]he secrecy shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks*.”).

E. The government’s public disclosures belie its blanket claims of secrecy and require disclosure of comparable Section 702 and FISA materials here.

In this case, as in every other FISA case over the past forty years, the Attorney General made the boilerplate claim that no shred of FISA-related material could be disclosed to the defense. V1 at 848. Here, however, this claim is belied by the government’s extensive disclosures of information concerning FISA surveillance—including information substantially similar to the information sought by Mr. Muhtorov.

Although the government represented that disclosure of *any* Section 702 or FISA material to Mr. Muhtorov would harm national security, it has publicly

disclosed the following Section 702 and FISA materials without harm to national security:

- Multiple versions of Section 702 targeting and minimization procedures.²²
- Multiple versions of standard minimization procedures for traditional FISA surveillance.²³
- Certifications and affidavits filed by the Director of National Intelligence, Attorney General, and Directors of the NSA and FBI in support of Section 702 applications.²⁴
- Dozens of FISC opinions and orders concerning FISA and Section 702 surveillance.²⁵
- Numerous oversight and transparency reports concerning the use of FISA authorities, including reports from the Privacy and Civil Liberties Oversight Board, Annual Statistical Transparency Reports, and Inspector General reports.²⁶
- The FISA application and renewals for the surveillance of Carter Page.²⁷

²² See, e.g., NSA Section 702 Minimization Procedures (2011), <https://bit.ly/2KL3Bzp>; FBI Section 702 Targeting Procedures (2015), <https://bit.ly/2LOvuJS>.

²³ See, e.g., FBI Standard Minimization Procedures for FISA Electronic Surveillance & Physical Search (2008), <https://bit.ly/2PbYWvK>.

²⁴ See, e.g., Certification of DNI & Attorney General Pursuant to FISA Subsection 702(g) (July 2015), <https://bit.ly/2KmCMBx>; Affidavit of Admiral Michael Rogers, Director, NSA (July 2015), <https://bit.ly/3387jLR>.

²⁵ See generally ODNI, IC on the Record, <https://bit.ly/30AiT0t>.

²⁶ See generally *id.*

²⁷ *In re Carter W. Page*, Verified Application to the FISC (Oct. 2016), <https://bit.ly/2ONWuXp>.

Although some of these disclosures contain redactions, they show that the government's blanket claim of secrecy in this case was plainly exaggerated. That the government has publicly disclosed Section 702 procedures and a FISA application is clear evidence that its withholding of comparable materials from Mr. Muhtorov, in their entirety, cannot be justified. Due process does not permit the government to withhold critical information from Mr. Muhtorov where disclosure would not genuinely threaten harm to national security. *See Roviato*, 353 U.S. at 60.

* * *

Accordingly, Mr. Muhtorov respectfully requests that this Court order disclosure of the Section 702 and FISA materials to defense counsel, under appropriate security precautions, because they are "necessary" to determining the lawfulness of the surveillance under Sections 1806(f) and 1825(g). At the very least, these materials cannot be withheld from Mr. Muhtorov in their entirety given that the government has repeatedly disclosed similar information without harm to national security.

The case should be remanded for additional disclosure, so that Mr. Muhtorov may supplement his motions to suppress and so that the district court may consider the lawfulness of these complex surveillance techniques with the benefit of informed adversarial briefing.

III. Beyond Section 702 and FISA, Mr. Muhtorov is entitled to notice of other novel surveillance tools used in the government’s investigation.

In recent years, the government has relied on an array of novel surveillance tools—not only Section 702 and traditional FISA surveillance—to warrantlessly monitor the communications and activities of investigative targets. Under various authorities, it has seized Americans’ phone records and financial data in bulk, deployed “stingrays” to track cell phones, secretly implanted malware on personal computers, and conducted sweeping internet surveillance. Yet the government often seeks to conceal these novel tools from criminal defendants subjected to them.

Here, the government refused to address two key questions about its monitoring of Mr. Muhtorov: What types of surveillance preceded the Section 702 and FISA surveillance in this case? And what *other* techniques did agents use alongside that surveillance?

The government’s insistence on complete secrecy is incompatible with the rights of defendants in the face of rapidly advancing technology. Indeed, the Supreme Court’s decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (prohibiting warrantless collection of cell-site location information), and the Second Circuit’s decision in *Clapper*, 785 F.3d 787 (prohibiting bulk collection of phone records), show why adversarial litigation is essential when it comes to surveillance. Without notice of the novel surveillance tools that the government

used in its investigation, Mr. Muhtorov was unable to challenge their lawfulness—and to seek suppression of the resulting evidence—even though those tools may well violate the Fourth Amendment.

Due process requires notice of surreptitious electronic surveillance in criminal cases because meaningful challenges are impossible without it.

Defendants are entitled to know how the government monitored their communications and activities, and then to test—in an adversarial proceeding—whether the government’s evidence is derived from that surveillance.

Yet the government has sought to carve out an exception to this due process requirement by misusing the Classified Information Procedures Act (“CIPA”). The government has used CIPA to completely preempt suppression litigation by making secret, one-sided claims that downplay the role of controversial surveillance techniques. Those arguments, however, are incompatible with CIPA itself and with controlling Supreme Court precedent, which requires adversarial litigation of core Fourth Amendment questions.

A. Preservation and standard of review.

Mr. Muhtorov’s motion for notice of the government’s surveillance techniques and objection to the government’s improper use of CIPA were raised below. V1 at 1126 (motion for notice); V3 at 448 (renewed motion); V3 at 481 (CIPA objection); V6 at 197 (CIPA and notice reply). The district court denied the

motion for notice and CIPA objection without explanation. V13 at 716. This Court reviews de novo the legal question of whether Mr. Muhtorov is entitled to notice, including his claim that Fourth Amendment suppression issues must be litigated in an adversarial proceeding. *United States v. Carr*, 939 F.2d 1442, 1443 (10th Cir. 1991); *United States v. Lustyik*, 833 F.3d 1263, 1267 (10th Cir. 2016).

B. The government refused to disclose the novel surveillance tools, beyond Section 702 and FISA, used to investigate Mr. Muhtorov.

Though much remains hidden from the defense, the record in this case leaves no doubt that Mr. Muhtorov was subject to multiple kinds of intrusive surveillance: agents searched Mr. Muhtorov’s email communications, logged his internet browsing, recorded his telephone calls, tracked his physical location, and examined his financial transactions. *See supra* Statement of Facts. But the government refused to disclose how it obtained much of this evidence. The government also refused to turn over an unknown number of defendants’ communications, which it obtained using an undisclosed set of surveillance techniques. *See, e.g.*, V7 at 343 (ruling on motion for discovery).

Some of the government’s surveillance in this case was conducted pursuant to FISA orders, but certainly not all of it. Investigations do not begin with FISA surveillance. Rather, as in other cases, the government’s FISA surveillance was undoubtedly the product of a pre-existing investigation. *See* Testimony of James Baker, former FBI General Counsel, at 68-71 (FISA surveillance “is not typically

the first thing[] that is done in an investigation. You build up to that point. You collect other information . . . and develop your probable cause.”).²⁸

Mr. Muhtorov describes some of the tools the government likely used here:

Executive Order 12,333. The government employs a panoply of powerful and controversial surveillance tools under Executive Order 12,333.²⁹ Unlike Section 702 surveillance, E.O. 12,333 surveillance typically occurs outside the United States. Using this authority, the NSA intercepts the contents and records of phone calls, video chats, emails, internet activity, and text messages—often in bulk, and all without a warrant. Because Americans routinely communicate with people and organizations located overseas, their communications are swept up in large quantities.³⁰

E.O. 12,333 is relevant here because the government appears to have closely monitored Mr. Muhtorov’s internet communications, Skype calls, and phone calls with individuals overseas. V1 at 180-85. Moreover, it has grown increasingly clear

²⁸ Executive Session, Committees on Judiciary and Government Reform & Oversight, U.S. House of Representatives (Oct. 3, 2018), <https://bit.ly/2OYKGMp>.

²⁹ E.O. 12,333, as amended, *available at* <https://bit.ly/2GNTqqq>.

³⁰ *See, e.g.*, Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014, <https://nyti.ms/2L9cROa> (“Savage 12,333 Article”); John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, <http://wapo.st/1wPuzv2>.

that FBI agents and NSA analysts use E.O. 12,333 information when investigating individuals in the United States.³¹

Notably, the Department of Justice believes it has no legal obligation to provide notice in criminal prosecutions when its evidence is the fruit of E.O. 12,333 surveillance.³² That seems to be the government's position in this case: it did not deny using E.O. 12,333 surveillance to monitor Mr. Muhtorov's activities, but it appears to have used a series of secret, one-sided filings to argue that Mr. Muhtorov should have no chance to challenge or even know about that surveillance. V5 at 205; V3 at 594.

Location-tracking. The government also appears to have collected information about Mr. Muhtorov's location, seemingly for months at a time, as he criss-crossed the country for work. V1 at 182 (describing Muhtorov's work-related travel to several states throughout 2011). The government never disclosed how it monitored Mr. Muhtorov's location at the various stages of its investigation, but the list of possibilities is long. Agents may have collected Mr. Muhtorov's cell-site location information ("CSLI"), conducted real-time GPS tracking, or deployed

³¹ See *Two Sets of Rules for Surveillance*, N.Y. Times, Aug. 13, 2014, <http://nyti.ms/1u2juDt> (chart describing uses of E.O. 12,333 surveillance); Ryan Gallagher, *The Surveillance Engine*, Intercept, Aug. 25, 2014, <http://bit.ly/1A1VFLL>.

³² Savage 12,333 Article.

“stingray” devices or “IMSI-catchers” to imitate cell towers.³³ All of these tools present distinct Fourth Amendment problems.

Yet the government has often sought to conceal its use of warrantless location-tracking techniques in court. For instance, the government long refused to tell defendants about its use of stingrays, while using euphemisms in court filings (like “tip,” “lead,” and “confidential source”) to hide or obscure the role of the devices, even from judges.³⁴ Although the government argued in this case that it could conceal *any* warrantless collection of records held by third parties—including, presumably, Mr. Muhtorov’s CSLI—that position is untenable after the Supreme Court’s decision in *Carpenter*. Compare V5 at 203, with *Carpenter*, 138 S. Ct. at 2216-17 (recognizing that individuals have a protected privacy interest in CSLI held by third parties).

Section 215. The government also obtained Mr. Muhtorov’s phone records, financial records, and subscriber information related to Mr. Muhtorov’s cell phone. *See, e.g.*, V1 at 180 (agents used “legally authorized methods” to determine Mr.

³³ Devlin Barrett, *Americans’ Cellphones Targeted in Secret U.S. Spy Program*, Wall St. J., Nov. 13, 2014, <https://on.wsj.com/2L0nXWH>; Devlin Barrett, *CIA Aided Program to Spy on U.S. Cellphones*, Wall St. J., March 10, 2015, <https://on.wsj.com/30EUbw1>.

³⁴ *See, e.g.*, Sam Adler-Bell, *Beware the ‘Stingray,’* U.S. News & World Report, Mar. 13, 2015, <http://bit.ly/1NT1RQ3>; Kim Zetter, *Emails Show Feds Asking Florida Cops to Deceive Judges*, Wired, June 19, 2014, <http://wrd.cm/SX0LKo>.

Muhtorov's phone number and model); V7 at 197-200. It may have done so through Section 215 of the Patriot Act, 50 U.S.C. § 1861.

The government has deployed a variety of novel surveillance tools under Section 215 to collect sensitive communications and financial records. The best-known program is the NSA's bulk collection of Americans' call records, which operated while agents were investigating Mr. Muhtorov. Through this program, the government served multiple companies with secret court orders requiring them to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating to every call placed on their networks.³⁵ The government routinely relied on its call-records database in criminal investigations, and it was permitted to freely query the database using phone numbers subject to a FISA order.³⁶ Here, the government refused to disclose whether agents obtained or queried Mr. Muhtorov's phone records, financial records, or other information using Section 215. *See* V5 at 203.

* * *

³⁵ Secondary Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc.*, No. BR 13-80 (FISC Apr. 25, 2013), <http://bit.ly/1vvXvXG>.

³⁶ *See* Order at 13, *In re Prod. of Tangible Things From [Redacted]*, No. BR 08-13 (FISC Mar. 2, 2009), <http://bit.ly/1rJup07>; Primary Order at 8-9, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 11-07 (FISC Jan. 20, 2011), <https://perma.cc/6GQD-G234>.

These examples are illustrative, not exhaustive. Because the government withheld even basic information about its surveillance, Mr. Muhtorov moved for notice, seeking among other things: (1) the surveillance techniques agents used in their investigation; (2) the legal authorities they relied upon; and (3) the nature and volume of data collected, including whether data was collected in bulk. V3 at 450.

For the reasons below, in denying this motion and related motions, the district court erred. *See* V13 at 716.

C. Recent decisions show that notice and adversarial litigation of Fourth Amendment questions is essential in an era of rapidly advancing technology.

The district court failed to require notice of two forms of surveillance—warrantless location-tracking and bulk collection of phone records—that other courts have recently found illegal. Given those decisions, there can be no question that Mr. Muhtorov is entitled to notice and the opportunity to raise similar challenges. These cases also show why adversarial litigation of surveillance tools is essential in an era of rapidly advancing technology.

In *Carpenter*, 138 S. Ct. at 2216-17, the Supreme Court recognized that individuals have a protected privacy interest in a new type of personal data: the cell-site location information generated by their mobile phones. The government for years insisted that the third-party doctrine foreclosed any Fourth Amendment challenge—and it repeatedly persuaded courts to approve the surveillance with less

than a warrant. Citing technological advances, the Supreme Court ultimately ruled otherwise. It did so, however, only with the benefit of extensive adversarial briefing on the technical details of the surveillance and the Fourth Amendment implications. *See id.* at 2217-18. *Carpenter* would have been unthinkable without adequate notice and disclosure to the defendant.

The same lesson emerges from the government's Section 215 surveillance. In *Clapper*, 785 F.3d at 822-24, the Second Circuit held that the NSA's bulk collection of Americans' call records was illegal. Although the FISC had approved the surveillance in secret for years, the outcome was markedly different in the face of adversarial litigation. The Second Circuit concluded that the suspicionless collection of Americans' call records violated the terms of Section 215 itself. *Id.*

Mr. Muhtorov is entitled to notice and the opportunity to raise similar arguments here, whether agents used warrantless location-tracking or Section 215 (or any other undisclosed method) to monitor his movements and activities.

D. Mr. Muhtorov is entitled to notice of the government's surveillance tools.

The Constitution, statutory law, and the Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice of the surveillance techniques that contributed to the government's investigation.

1. The Fourth and Fifth Amendments entitle Mr. Muhtorov to notice of the government’s surveillance techniques.

Notice of the government’s surveillance techniques is essential to Mr. Muhtorov’s due process rights. As explained above, due process requires that criminal defendants have a meaningful opportunity to suppress the fruits of illegally acquired evidence. *See, e.g., supra* Part II.D; *see also Jencks v. United States*, 353 U.S. 657, 671 (1957) (the government cannot invoke its privileges to “deprive the accused of anything which might be material to his defense”); *Keith*, 407 U.S. at 318-24 (compelling disclosure of surveillance transcripts in a national security case); *Alderman*, 394 U.S. at 180-88 (same).

Notice of surveillance was not only material to Mr. Muhtorov’s defense—it was indispensable. To seek suppression, Mr. Muhtorov must, at a minimum, be aware of the surveillance that contributed to the government’s investigation.

Indeed, courts have long found that notice is a constitutionally required element of surreptitious searches like wiretaps and sneak-and-peek entries. *See Berger*, 388 U.S. at 60 (finding wiretapping statute unconstitutional because, among other things, it had “no requirement for notice”); *Dalia*, 441 U.S. 238, 247-48 (Title III provides “a constitutionally adequate substitute for advance notice” by requiring notice after the surveillance is completed (emphasis added)); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peek

warrant constitutionally defective for its failure to provide notice within a reasonable time).

2. 18 U.S.C. § 3504 entitles Mr. Muhtorov to notice of the government’s surveillance techniques.

Recognizing the dangers of surreptitious surveillance, Congress also provided a right to notice of surveillance by statute. Under 18 U.S.C. § 3504(a), if a party in a proceeding before any court claims that “evidence is inadmissible” because “it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act,” then the government must “affirm or deny the occurrence of the alleged unlawful act.” The statute defines “unlawful act” as “the use of any electronic, mechanical, or other device” in violation of the law. *Id.* § 3504(b).

Thus, Section 3504 requires “the affirmance or denial of the *fact* of electronic surveillance, even if the government believes it was lawful.” Kris & Wilson, 2 *National Security Investigations & Prosecutions* § 27:12 (2d ed. 2012). A “cognizable claim” for notice under the statute “need be no more than a ‘mere assertion’” that illegal surveillance has taken place. *United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (citation omitted). The party must make a prima facie showing that he was “aggrieved” by the surveillance, which need only have a “colorable basis.” *Id.*

Mr. Muhtorov has made such a showing with respect to several different types of surveillance. *See* V1 at 1126, 1152. For these reasons, Section 3504 requires notice of the surveillance methods used in this case.³⁷

3. The Federal Rules of Criminal Procedure entitle Mr. Muhtorov to notice of the government’s surveillance techniques.

The Federal Rules of Criminal Procedure also support Mr. Muhtorov’s request for notice. Under Rule 16(a)(1)(B), Mr. Muhtorov is expressly entitled to discovery of his relevant recorded statements. *See* V5 at 524-30. And under Rule 16(a)(1)(E), Mr. Muhtorov is entitled to items “obtained from or belong[ing] to” him, as well as information “material to preparing the defense.” *See id.* Because notice of the government’s surveillance techniques is essential to Mr. Muhtorov’s ability to seek suppression, this information is plainly “material” under Rule 16(a)(1)(E)(i). *See United States v. Soto-Zuniga*, 837 F.3d 992, 1000-01 (9th Cir. 2016).

³⁷ Below, the government cursorily “denie[d] that any evidence to be admitted at trial was the primary product of, or was obtained by the exploitation of, surveillance conducted pursuant to Executive Order 12,333 as to which defendants are aggrieved.” V5 at 205. But Section 3504 does not permit the government to condition disclosure based on its own claims about whether the evidence was tainted. *See Matter of Grand Jury*, 524 F.2d 209, 216 (10th Cir. 1975) (“[I]f the government’s position is to be denial, it should be given in absolute terms[.]”).

E. The government’s use of CIPA to conceal novel surveillance of Mr. Muhtorov violated both CIPA and due process.

The unclassified record strongly suggests that the district court allowed the government to conceal novel surveillance techniques through CIPA, 18 U.S.C. app. III. This violated both the CIPA framework and due process, which requires adversarial litigation of Fourth Amendment suppression issues—especially in cases involving complex surveillance.

CIPA’s fundamental purpose is to regulate the discovery and use of classified information in a way that does not impair the defendant’s right to due process. Under Section 4 of CIPA, courts apply a three-step procedure to determine whether classified, arguably discoverable information must be disclosed to the defense. They determine whether the material is (1) discoverable under the ordinary rules of criminal discovery; (2) in fact privileged; and (3) “at least helpful to the defense.” *United States v. Hanna*, 661 F.3d 271, 295 (6th Cir. 2011). If the court concludes that the material is at least helpful, then it must be disclosed, though the court may impose conditions to safeguard sensitive information. *See United States v. Rezaq*, 134 F.3d 1121, 1142-43 (D.C. Cir. 1998).

As discussed below, information concerning the government’s surveillance of Mr. Muhtorov in its investigation is plainly relevant and helpful, and should have been disclosed to the defense.

Yet the district court, relying on CIPA, apparently allowed the government to shield its novel surveillance tools from disclosure. In response to Mr. Muhtorov’s motion to compel notice, the district court stated that it would address the issue once CIPA proceedings were concluded. *See* V11 at 268. When Mr. Muhtorov objected to the improper use of CIPA, the government filed a vague non-denial, stating: “the CIPA pleadings in this case related only to summarizing, substituting, or deleting individual products of discovery. . . . For this reason, the government does not address the legal arguments discussed therein[.]” V3 at 594. That the government “only” sought to “delete” evidence says nothing about whether the deleted discovery was the fruit of undisclosed surveillance.

In rulings on motions for discovery brought by Mr. Muhtorov and Mr. Jumaev, the court also made clear that it was permitting the government to withhold defendants’ recorded statements under CIPA. *See* V7 at 342-44; V13 at 390. For example, the court refused to order disclosure of Mr. Jumaev’s statements on the ground that they were “covered by the state-secrets privilege” and “irrelevant and unhelpful”—despite their obvious relevance and helpfulness to any motion to suppress. *See id.*; *see also* V13 at 415-16 (court stating that “a great deal of what is . . . protected by CIPA has to do with methodology,” and refusing to order disclosure).

While this case was pending, the Department of Justice Inspector General released a report publicly describing, for the first time, how the government was using CIPA's ex parte procedures to conceal surveillance in criminal cases.³⁸ The OIG Report concerns the warrantless "Stellar Wind" surveillance programs, which the government operated for years without congressional or judicial approval. *See* OIG Report 203-66. As the report explains, the government used CIPA to argue—ex parte—that surveillance materials were not discoverable, because defendants would not ultimately *succeed* in suppressing the government's evidence:

The government argued that because the facts concerning the NSA's reporting would not aid the defense, the court need not explore the sources and methods used to acquire the information. The submissions also argued that the information collected by the NSA was not included in the government's FISA application, and therefore was too attenuated from the trial evidence to merit a review of the means by which the intelligence information was gathered. The government asserted that the "causal connection" between discovery of the derivative evidence and the alleged illegal search "may have become so attenuated as to dissipate the taint."

OIG Report 351 (V3 at 525). In other words, the government invariably claimed that its evidence was not "tainted" by the warrantless surveillance, even though the OIG Report suggests otherwise. *See id.* at 271-331. The government thus concealed its use of Stellar Wind surveillance from every single criminal defendant

³⁸ DOJ Office of the Inspector General, *A Review of the Department of Justice's Involvement with the President's Surveillance Program* (July 2009) ("OIG Report"), <https://bit.ly/2PkLV35> (excerpted at V3 at 507).

who was subject to it—ensuring that neither the surveillance nor the government’s “taint” claims were ever subject to challenge.

Here, for two reasons, the district court erred in permitting the government to similarly use CIPA to shield undisclosed surveillance from Mr. Muhtorov.

First, under the CIPA framework itself, information concerning the surveillance of Mr. Muhtorov should have been disclosed. This information is discoverable and per se relevant and helpful because it is a necessary predicate to any motion to suppress the government’s evidence as fruit of the poisonous tree. *See, e.g., supra* Part II.D; *United States v. Chun*, 503 F.2d 533, 536-37 & n.6 (9th Cir. 1974); *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008) (information is “helpful or material” if it is “useful to counter the government’s case or to bolster a defense,” and need not be “‘favorable’ in the *Brady* sense”). Moreover, CIPA “does not expand or restrict established principles of discovery,” *Sedaghaty*, 728 F.3d at 903—including Mr. Muhtorov’s rights to disclosure.

Second, due process does not permit the government to litigate Fourth Amendment suppression issues entirely in secret under the guise of “relevance.” As the Supreme Court has made clear, Fourth Amendment suppression questions are notoriously fact-specific and complex—and must be resolved through disclosure and adversarial litigation.

In *Alderman v. United States*, the Supreme Court held that defendants must be permitted to discover information that may be relevant to whether the government's evidence is fruit of the poisonous tree, because only an adversarial process can ensure fair and accurate resolution of this Fourth Amendment issue. 394 U.S. at 168, 180-85. Emphasizing the difficult judgments raised by "cases involving electronic surveillance," the Court said, "in our view the task is too complex, and the margin for error too great, to rely wholly on the in camera judgment of the trial court." *Id.* at 182 & n.14. Instead, to avoid leaving the trial court and defendants entirely reliant on the government's one-sided claims, adversarial proceedings are necessary "to provide the scrutiny which the Fourth Amendment exclusionary rule demands." *Id.* at 184; *see also Trujillo v. Sullivan*, 815 F.2d 597, 616 (10th Cir. 1987); *Nolan v. United States*, 423 F.2d 1031, 1041 (10th Cir. 1969) ("[A]fter alleging the existence of illegal surveillance . . . the defendant was entitled to inspect all recordings and transcripts made of his conversations[.]").³⁹

³⁹ Courts applying *Alderman* have permitted *ex parte* review as to certain questions concerning how *much* disclosure of surveillance is required, such as whether a given recording contains a defendant's voice. *See Taglianetti v. United States*, 394 U.S. 316, 317 (1969). But the same cases show that Mr. Muhtorov is entitled to notice of the surveillance itself, and an opportunity to litigate suppression. *See id.*; *United States v. Villano*, 529 F.2d 1046, 1056-59 (10th Cir. 1976) (transcripts of wiretaps disclosed and adversarial taint hearing conducted).

The lesson of *Alderman* and its progeny is that defendants are entitled to notice of surveillance, *despite* the government’s unilateral claims that the information is not “relevant or helpful,” that an exception to the fruit-of-the-poisonous-tree doctrine should apply, or that its surveillance was lawful. *See, e.g., Kolod v. United States*, 390 U.S. 136 (1968) (per curiam) (rejecting the government’s unilateral determination that evidence was not derived from challenged surveillance and requiring adversarial proceedings); *United States v. Alderisio*, 424 F.2d 20, 23 (10th Cir. 1970) (district court erred in denying as immaterial defense requests to examine FBI memoranda concerning surveillance of defendant); *Apple*, 915 F.2d at 910-11 (district court abused its discretion in addressing an exception to the fruit-of-the-poisonous-tree doctrine before the government adequately addressed alleged surveillance).

* * *

In its effort to withhold surveillance evidence under CIPA, the government may have advanced a number of arguments addressing fundamental Fourth Amendment issues. For example, as the OIG Report suggests, it may have argued that: (1) the surveillance was “too attenuated” from the trial evidence; (2) the surveillance was merely a “tip” or a “lead”; (3) the FISA applications broke the causal chain; (4) the trial evidence was obtained from an “independent” source; or (5) the “inevitable discovery” exception applied. But as the Supreme Court and this

Court have made clear, these are complex questions that should not and cannot be litigated *ex parte*. Regardless of which theories the government advanced in secret below, it is plain that it used CIPA proceedings to withhold basic information about the surveillance of Mr. Muhtorov—information relevant and helpful to a motion to suppress. The district court erred by refusing to order notice.

Because Mr. Muhtorov does not have access to the *ex parte* record, he does not know where in that record the government's surveillance techniques are addressed. But to facilitate the *de novo* review required here, the Court should begin with a complete and accurate picture of the surveillance actually used in this case. Accordingly, Mr. Muhtorov respectfully requests that the Court:

(1) Direct the government to identify the portions of the *ex parte* record addressing the government's surveillance of Mr. Muhtorov;

(2) Closely review the government's FISA applications to identify which surveillance techniques contributed to them; and

(3) Require the government to identify, with specificity, the various types of surveillance that agents used in their investigation of Mr. Muhtorov, including how agents obtained the communications of his that the government withheld in discovery.⁴⁰

⁴⁰ Clarity as to the surveillance techniques actually used is essential, given reports that controversial techniques may be omitted, obscured, or vaguely described in court filings. *See* John Shiffman & Kristina Cooke, *U.S. Directs*

Following this review, the Court should order disclosure to defense counsel, under appropriate security measures, of the surveillance techniques agents used in their investigation; the legal authorities they relied upon; and the nature and volume of data collected. The case should then be remanded, so that Mr. Muhtorov may challenge the government's novel surveillance techniques and seek suppression accordingly.

IV. The nearly six-and-a-half-year delay between Mr. Muhtorov's arrest and trial violated his constitutional right to a speedy trial.

The government took nearly six and a half years to bring Mr. Muhtorov to trial. A man with no criminal history, he spent every day of that time in pretrial detention, deprived of contact with his family. His mental health deteriorated, and by the time he went to trial, an important defense witness had died. The blame for this delay falls squarely at the government's feet, which it dragged at every turn. Ultimately, this delay violated Mr. Muhtorov's Sixth Amendment speedy trial right, a right he invoked repeatedly.

Mr. Muhtorov's co-defendant, Mr. Jumaev, also waited over six years for trial, and he similarly challenges that delay as violating his constitutional speedy

Agents to Cover Up Program Used to Investigate Americans, Reuters, Aug. 5, 2013, <http://reut.rs/1h07Hkl>; Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Wash. Post, Feb. 22, 2015, <https://wapo.st/1K7cKfX>.

trial right. (Opening Br., 18-1296, Issue I). His arguments are, in large measure, equally applicable to Mr. Muhtorov. Rather than repeat them, Mr. Muhtorov joins in Mr. Jumaev's constitutional speedy trial claim pursuant to Fed. R. App. P. 28(i). He writes separately, however, to explain how those arguments apply to him, and to identify some facts unique to his case. *See United States v. Renteria*, 720 F.3d 1245, 1251 (10th Cir. 2013).

A. Preservation and standard of review.

Mr. Muhtorov's constitutional speedy trial challenge was raised and ruled upon below. V15 at 282 (motion to dismiss); V12 at 546 (denial); V15 at 522 (renewed motion); V20 at 147 (denial). This Court reviews de novo the legal question of whether there was a constitutional speedy trial violation. *United States v. Black*, 830 F.3d 1099, 1111 (10th Cir. 2016).

B. The *Barker v. Wingo* factors overwhelmingly favor Mr. Muhtorov.

As Mr. Jumaev explains, this Court's de novo review is guided by the four factors in *Barker v. Wingo*, 407 U.S. 514 (1972). Here, all four point decidedly in Mr. Muhtorov's favor.

1. Length of the delay

As with Mr. Jumaev (Part I.A), the over six-year delay between Mr. Muhtorov's arrest and trial satisfies *Barker's* first prong, and weighs heavily in Mr.

Muhtorov's favor. *See United States v. Seltzer*, 595 F.3d 1170, 1176 (10th Cir. 2010).

2. Reason for the delay

As Mr. Jumaev notes (at I.B), it is the government's burden to provide an acceptable rationale for its delays, and even negligence and neutral factors count against it. And, as he explains, the reasons for the delay here rest almost exclusively with the government.

The men were joined for trial from their arrests in 2012, until November 29, 2016, when the district court severed the cases. V1 at 90. As such, the delays Mr. Jumaev recounts prior to that time plainly impact Mr. Muhtorov as well. But even post-severance, the two cases moved along parallel paths, with most court hearings held jointly, and many motions jointly pursued. V1 at 90-137. Accordingly, Mr. Juamev's recounting of the government's administrative failures, its discovery delays, and its addition and subsequent dismissal of counts 5 and 6, all apply with equal force to Mr. Muhtorov. As to him specifically, two additional points warrant brief mention:

The government's belated Section 702 notice. The district court observed in 2017 that the Section 702 suppression litigation delayed the trial. V7 at 14. But that delay doesn't count against Mr. Muhtorov in the slightest here, because that litigation could have been completed far earlier. The only reason it wasn't is that

the government waited until “nearly two years after Mr. Muhtorov’s arrest” to provide notice that it had employed Section 702 in his case. V3 at 116-22. Notably, that’s about the same amount of time that elapsed between Mr. Muhtorov’s suppression motion and the district court’s denial. V1 at 666; V3 at 115.

Post-severance discovery delays. Even after the men’s trials were severed, delays unique to Mr. Jumaev’s case continued to impact Mr. Muhtorov. That’s because the severance was predicated on Mr. Muhtorov being tried second. V12 at 553, V15 at 284-86. But when the court continued Mr. Jumaev’s scheduled March 2017 trial by nine months (on the morning of trial, and due to the government’s discovery delays), it did so without consideration of its impact on Mr. Muhtorov, noting that “we’ll figure out what to do with [him].” Doc. 1382 at 80.⁴¹ What was “figure[d] out,” ultimately, was that Mr. Muhtorov had to accede to moving his trial to preserve the possibility of calling Mr. Jumaev as a witness—an intolerable choice of surrendering one constitutional right in order to assert another. V12 at 552-54. So instead of being tried in July 2017, his trial was reset to March 2018, and then, following another delay due to a personal issue of the court, to May 2018—nearly another year later. V13 at 1078-89. In this way, then, even discovery

⁴¹ Mr. Muhtorov will supplement the record with materials from the proceedings below that bear on this claim, but which are not currently part of the appellate record.

delays unique to Mr. Jumaev caused delays for Mr. Muhtorov, and weigh against the government here.

3. Invocation of the right

Like Mr. Jumaev (at Part I.C), Mr. Muhtorov continuously asserted his right. He twice moved through counsel to dismiss the indictment for constitutional speedy trial violations (*supra* Part IV.A), and repeatedly sought similar relief in pro se filings. V1 at 113-14 (Docs. 1402, 1405); V15 at 305. Along with Mr. Jumaev, he voiced objections with the slow pace of the government’s discovery efforts throughout the proceedings. *E.g.*, V7 at 303; V15 at 293-94; V17 at 41, 58. Simply put, Mr. Muhtorov made clear that he wished for a prompt resolution of his case, and this factor also favors him.

4. Prejudice

Finally, as with Mr. Jumaev (Part I.D), Mr. Muhtorov’s six-and-a-half-year wait presents a case of “extreme” delay under *Doggett v. United States*, 505 U.S. 647 (1992). Accordingly, he need not make specific showings of prejudice, but can instead rely on a presumption of prejudice resulting from the prolonged delay. *United States v. Medina*, 918 F.3d 774, 780 (10th Cir. 2019) (“Generally, the court requires a delay of six years before allowing the delay itself to constitute prejudice.”). That presumption alone is enough for him to prevail. But even if Mr.

Muhtorov must make individualized showings of prejudice, he can do so in each of the three ways this Court has identified. *Id.* at 781.⁴²

a. Oppressive pretrial incarceration

As an Uzbek- and Russian-speaking Muslim, Mr. Muhtorov's time in custody was neither typical, nor easy. The problems began as early as his arrest, with counsel noting at Mr. Muhtorov's arraignment that he'd been placed in 24-hour lockdown, with no access to a telephone, or religious or other reading materials. Doc. 56 at 10. It appears to have taken two months for the issue to be resolved, and only with "extrajudicial" intervention of the district court. V12 at 569. Over the years, he spent time at numerous facilities. V18 at 441. Similar problems appear to have reoccurred, and, additionally, these facilities didn't permit contact visits, so Mr. Muhtorov spent years without any physical interaction with his family. His youngest child was born shortly after his arrest, and for the first six years of her life, Mr. Muhtorov never held her, and saw her only through the glass barriers of a jail's visiting room. V14 at 23-24; V19 at 39-40; V20 at 1345, 1352.

⁴² The district court appears to have applied the presumption of prejudice (V20 at 148-49), and concluded that the first, third, and fourth *Barker* factors favored Mr. Muhtorov (*id.*; V12 at 547-54). But it declined to find a constitutional violation because, in its view, the second prong favored the government. (*Id.*, V20 at 150) But as Mr. Jumaev explains, that conclusion is wrong; the second prong actually weighs in both defendants' favor.

His experience was well beyond the norm—substantively and temporally. Indeed, as the Second Circuit recognized last year, “[n]early seven years of pretrial detention in local jails—before the defendant has been convicted of any crime—is precisely the type of prejudice contemplated by the right to a speedy trial.” *United States v. Tigano*, 880 F.3d 602, 618 (2d Cir. 2018).

b. Anxiety and concern

This Court requires a defendant to “show some special harm which distinguishes [his] case” from the harms attendant with “any other arrestee awaiting trial.” *United States v. Frias*, 893 F.3d 1268, 1273 (10th Cir. 2018). Mr. Muhtorov can make that showing.

About five years into his pretrial detention, Mr. Muhtorov disclosed to the jail’s medical staff significant struggles “emotionally [and] physically, with being locked up.” A case worker remarked that he “continues to not look like he is coping well,” and for the first time in his life, he was prescribed medication for depression and anxiety. V18 at 457. The district court showed little surprise at this, remarking later that “I can well understand somebody who has been confined for six years is going to have mental problems.” V14 at 25.

c. Impairment of defense

Impairment of the defense can take many forms, but “[i]f witnesses die or disappear during a delay, the prejudice is obvious.” *Barker*, 407 U.S. at 532. That’s

what happened here. One of the defense's key witnesses was Vasila Inoyatova, a prominent human rights activist in Uzbekistan. But she died just weeks before she was scheduled to testify at trial. V15 at 522-28.

When evaluating whether the loss of evidence amounts to speedy-trial prejudice, this Court looks to three factors, *Medina*, 918 F.3d at 781-83, each of which is satisfied here:

(1) *The defendant's ability to demonstrate with specificity how the evidence would have aided his defense.* Mr. Muhtorov renewed his speedy trial motion after Ms. Inoyatova's death, proffering that her testimony would have covered the human rights work Mr. Muhtorov and others did in Uzbekistan, and the continuing oppression in the years that followed—factors that were critical aspects of his defense. *Id.* at 522-28.

(2) *Whether the government's delay caused the evidence to be actually lost.* Here, Ms. Inoyatova's death occurred after the one-year mark triggering the speedy trial inquiry, but before Mr. Muhtorov was tried. *See Jackson v. Ray*, 390 F.3d 1254, 1265-66 (10th Cir. 2004). There can be little question then that, but for the delay, Ms. Inoyatova would have been available to testify; instead, her testimony was, quite plainly, "irretrievable." *Medina*, 918 F.3d at 782.

(3) *Whether the defendant took appropriate steps to preserve the evidence.* Getting Ms. Inoyatova from Uzbekistan to the U.S. required special approvals,

which defense counsel worked to obtain. V4 at 707, 746, 782. Beyond that, there was no reason to think that her testimony needed to be preserved. She corresponded with counsel shortly before her death, indicating that she looked forward to testifying, and then died suddenly shortly thereafter. V15 at 527.

Under these circumstances then, the delay impaired Mr. Muhtorov's defense.

* * *

In 2017, this Court affirmed the procedural dismissal of a pro se filing by Mr. Muhtorov asserting speedy trial claims. *Muhtorov v. Choate*, 697 F. App'x 608, 609 (10th Cir. 2017) (unpublished). In doing so, it remarked that "the length of the delay in this case is troubling." Indeed, it was; and even more so when his case finally went to trial the following year.

Barker's factors are a balancing test, but here that balance weighs entirely on one side, and leads inexorably to the conclusion that Mr. Muhtorov was denied a speedy trial. For these reasons, this Court should reverse the district court's decision, vacate Mr. Muhtorov's convictions, and remand with instructions to dismiss the indictment with prejudice, which is "the only possible remedy."

Barker, 407 U.S. at 522.

CONCLUSION

For these reasons, Mr. Muhtorov respectfully requests that this Court vacate his convictions and either remand this case with instructions to dismiss the indictment (Issue IV) or for further proceedings (Issues I, II, and III).

STATEMENT REGARDING ORAL ARGUMENT

This case presents three questions of first impression in this circuit. The proceedings below spanned over six and a half years, now comprising over 2,000 docket entries, and the appellate record is extremely large, at over 12,000 pages. Accordingly, counsel believe oral argument will assist the court in adjudicating the issues presented, and therefore request the opportunity to present argument.

Respectfully submitted,

VIRGINIA L. GRADY
Federal Public Defender

/s/ John C. Arceci

JOHN C. ARCECI
Assistant Federal Public Defender
633 17th Street, Suite 1000
Denver, Colorado 80202
(303) 294-7002
Email: John_Arceci@fd.org
COX_10ecf@fd.org

/s/ Patrick Toomey

PATRICK TOOMEY
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500
Email: ptoomey@aclu.org

/s/ Ashley M. Gorski

ASHLEY M. GORSKI
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500
Email: agorski@aclu.org

Counsel for Appellant Jamshid Muhtorov

**CERTIFICATES OF COMPLIANCE,
DIGITAL SUBMISSION, AND SERVICE**

As required by Fed. R. App. P. 32(g)(1), and consistent with this Court's Orders of August 14, 2019 and August 28, 2019, granting in part Mr. Muhtorov's motion to exceed the word count provided under Fed. R. App. P. 32(a)(7), I certify that the foregoing *Appellant's Opening Brief* is proportionally spaced, set in Times New Roman font, size 14, and contains 21,178 words. I relied on my word processor, Microsoft Word 2016, to obtain the count. I certify that the information on this form is true and correct to the best of my knowledge and belief formed after a reasonable inquiry.

I hereby certify that with respect to the foregoing *Appellant's Opening Brief*, (1) all required privacy redactions have been made; (2) the ECF submission is an exact copy of the filed hard copy; and (3) the ECF submission was scanned for viruses with Symantec Endpoint Protection version 14.2.3332.1000, Virus Definition File dated Monday, September 30, 2019, 2019 r3, and, according to the program is free of viruses.

I hereby certify that consistent with this Court's Order of August 29, 2019, on September 30, 2019, I electronically filed the foregoing *Appellant's Opening Brief* using the CM/ECF system, which will send notification of this filing to James C. Murphy, Assistant U.S. Attorney, at james.murphy3@usdoj.gov. I further certify that that I also will send a copy of this filing by email to Caleb Kruckenberg, Counsel for Appellant Bakhtiyor Jumaev, at caleb.kruckenberg@ncla.legal.

/s/ John C. Arceci

JOHN C. ARCECI

Assistant Federal Public Defender

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 1

Vol. 16: 247-253

UNITED STATES DISTRICT COURT

District of Colorado

UNITED STATES OF AMERICA

v.

JAMSHID MUHTOROV

JUDGMENT IN A CRIMINAL CASE

Case Number: 1:12-cr-00033-JLK-1

USM Number: 42383-424

Brian Rowland Leedy, Warren Richard Williamson,
 Jacob R. Rasch-Chabot, Kathryn J. Stimson, and
 Patrick C. Toomey

Defendant's Attorney

THE DEFENDANT:

- pleaded guilty to count(s) _____
- pleaded nolo contendere to count(s) _____
 which was accepted by the court.
- was found guilty on counts 1, 2 and 3 of the Second Superseding Indictment
 after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

<u>Title & Section</u>	<u>Nature of Offense</u>	<u>Offense Ended</u>	<u>Count</u>
18 U.S.C. § 2339B	Material Support of a Designated Foreign Terrorist Organization and Conspiracy and Attempt to do the Same	01/21/12	1
18 U.S.C. § 2339B	Material Support of a Designated Foreign Terrorist Organization and Conspiracy and Attempt to do the Same	01/21/12	2
18 U.S.C. § 2339B	Material Support of a Designated Foreign Terrorist Organization and Conspiracy and Attempt to do the Same	01/21/12	3

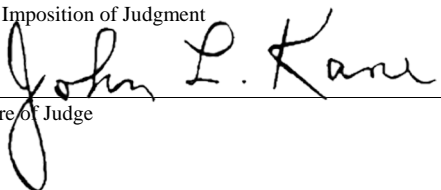
The defendant is sentenced as provided in pages 2 through 7 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

- The defendant has been found not guilty on counts 4 of the Second Superseding Indictment
- Count(s) _____ is are dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

August 30, 2018

Date of Imposition of Judgment



Signature of Judge

John L. Kane, Senior United States District Judge

Name and Title of Judge

September 4, 2018

Date

DEFENDANT: JAMSHID MUHTOROV
CASE NUMBER: 1:12-cr-00033-JLK-1

IMPRISONMENT

The defendant is hereby committed to the custody of the Federal Bureau of Prisons to be imprisoned for a total term of: **one hundred and thirty-two (132) months;** ninety-six (96) months as to Count 1, ninety-six (96) months as to Count 2, and one hundred and thirty-two (132) months as to Count 3, each Count to run concurrent.

- The court makes the following recommendations to the Bureau of Prisons:
The Court recommends the defendant be designated to a facility in Colorado, and that he receive credit for presentence confinement of 2,413 days.
- The defendant is remanded to the custody of the United States Marshal.
- The defendant shall surrender to the United States Marshal for this district:
 - at _____ a.m. p.m. on _____ .
 - as notified by the United States Marshal.
- The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:
 - before 2 p.m. on _____ .
 - as notified by the United States Marshal.
 - as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____
at _____, with a certified copy of this judgment.

UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

DEFENDANT: JAMSHID MUHTOROV
CASE NUMBER: 1:12-cr-00033-JLK-1

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a term of: **fifteen (15) years**, each Count to run concurrent.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.
 - The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. *(check if applicable)*
4. You must make restitution in accordance with 18 U.S.C. §§ 3663 and 3663A or any other statute authorizing a sentence of restitution. *(check if applicable)*
5. You must cooperate in the collection of DNA as directed by the probation officer. *(check if applicable)*
6. You must comply with the requirements of the Sex Offender Registration and Notification Act (34 U.S.C. § 20901, *et seq.*) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in the location where you reside, work, are a student, or were convicted of a qualifying offense. *(check if applicable)*
7. You must participate in an approved program for domestic violence. *(check if applicable)*

You must comply with the standard conditions that have been adopted by this court as well as with any other conditions on the attached page.

DEFENDANT: JAMSHID MUHTOROV
CASE NUMBER: 1:12-cr-00033-JLK-1

STANDARD CONDITIONS OF SUPERVISION

As part of your supervised release, you must comply with the following standard conditions of supervision. These conditions are imposed because they establish the basic expectations for your behavior while on supervision and identify the minimum tools needed by probation officers to keep informed, report to the court about, and bring about improvements in your conduct and condition.

1. You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.
2. After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.
3. You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.
4. You must answer truthfully the questions asked by your probation officer.
5. You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
6. You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.
7. You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
8. You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.
9. If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.
10. You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).
11. You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.
12. If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.
13. You must follow the instructions of the probation officer related to the conditions of supervision.

U.S. Probation Office Use Only

A U.S. probation officer has instructed me on the conditions specified by the court and has provided me with a written copy of this judgment containing these conditions. For further information regarding these conditions, see *Overview of Probation and Supervised Release Conditions*, available at: www.uscourts.gov.

Defendant's Signature _____

Date _____

DEFENDANT: JAMSHID MUHTOROV
CASE NUMBER: 1:12-cr-00033-JLK-1

SPECIAL CONDITIONS OF SUPERVISION

1. If you are deported, you must not thereafter re-enter the United States illegally. If you re-enter the United States legally, you must report to the nearest U.S. Probation Office within 72 hours of your return.
2. You must not under any circumstance use, own, or operate any computer or similar device without written authorization by the probation officer, and you must allow the probation officer to install software/hardware designed to monitor computer activities on any computer you are authorized by the probation officer to use. The software may record any and all activity on the computer, including the capture of keystrokes, application information, internet use history, email correspondence, and chat conversations. A notice will be placed on the computer at the time of installation to warn others of the existence of the monitoring software on the computer. You must not attempt to remove, tamper with, reverse engineer, or in any way circumvent the software/hardware.
3. You must submit your person, property, house, residence, vehicle, papers, computers (as defined in 18 U.S.C. § 1030(e)(1)), other electronic communications or data storage devices or media, or office, to a search conducted by a United States probation officer. Failure to submit to search may be grounds for revocation of release. You must warn any other occupants that the premises may be subject to searches pursuant to this condition. An officer may conduct a search pursuant to this condition only when reasonable suspicion exists that you have violated a condition of your supervision and that the areas to be searched contain evidence of this violation. Any search must be conducted at a reasonable time and in a reasonable manner.
4. You shall not possess, view, access, or otherwise use material that reflects extremist or terroristic views or is deemed to be similarly inappropriate by the U.S. Probation Office.

DEFENDANT: JAMSHID MUHTOROV
CASE NUMBER: 1:12-cr-00033-JLK-1

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on the following page.

	<u>Assessment</u>	<u>JVTA Assessment*</u>	<u>Fine</u>	<u>Restitution</u>
TOTALS	\$ 300.00	\$ 0.00	\$ 0.00	\$ 0.00

- The determination of restitution is deferred until _____. An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.
- The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

<u>Name of Payee</u>	<u>Total Loss**</u>	<u>Restitution Ordered</u>	<u>Priority or Percentage</u>
----------------------	---------------------	----------------------------	-------------------------------

TOTALS	\$	\$
<input type="checkbox"/> Restitution amount ordered pursuant to plea agreement	\$	_____

- The defendant must pay interest on restitution and a fine of more than \$2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on the following page may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).
- The court determined that the defendant does not have the ability to pay interest and it is ordered that:
 - the interest requirement is waived for the fine restitution.
 - the interest requirement for the fine restitution is modified as follows:

* Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.

** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: JAMSHID MUHTOROV
CASE NUMBER: 1:12-cr-00033-JLK-1

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

- A Lump sum payment of \$ _____ due immediately, balance due
- not later than _____, or
- in accordance with C, D, E, or F below; or
- B Payment to begin immediately (may be combined with C, D, or F below); or
- C Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after the date of this judgment; or
- D Payment in equal _____ (e.g., weekly, monthly, quarterly) installments of \$ _____ over a period of _____ (e.g., months or years), to commence _____ (e.g., 30 or 60 days) after release from imprisonment to a term of supervision; or
- E Payment during the term of supervised release will commence within _____ (e.g., 30 or 60 days) after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or
- F Special instructions regarding the payment of criminal monetary penalties:

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

- Joint and Several

Defendant and Co-Defendant Names and Case Numbers (including defendant number), Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

- The defendant shall pay the cost of prosecution.
- The defendant shall pay the following court cost(s):
- The defendant shall forfeit the defendant's interest in the following property to the United States:

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) JVTAs assessment, (8) penalties, and (9) costs, including cost of prosecution and court costs.

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 2

Vol. 3: 115-149

(ISSUE I)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. JAMSHID MUHTOROV,
2. BAKHTIYOR JUMAEV,

Defendants.

ORDER DENYING MOTION TO SUPPRESS EVIDENCE OBTAINED OR
DERIVED UNDER FISA AMENDMENTS ACT OR FOR DISCOVERY (Doc. 520)

Kane, J.

Jamshid Muhtorov, together with his co-defendant Bakhtiyor Jumaev, is charged with providing material support to a designated terrorist organization, and attempt and conspiracy to do the same. His arrest on a one-way flight to Turkey was originally believed to be solely the result of warrantless surveillance and physical searches authorized under Title I and III of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801-1811, 1821-1829. Mr. Muhtorov moved to suppress that FISA-acquired evidence earlier in these proceedings, which motion I denied based on a determination, after an extensive *in camera* review of the classified materials submitted to the FISA Court, that there was probable cause to believe the target was an agent as described and

therefore lawfully subject to those searches.

The matter is before me on a renewed Motion to Suppress, precipitated by the government's supplemental disclosure, nearly two years after Mr. Muhtorov's arrest, that some of the FISA-acquired evidence it intends to use against him in this case was derived from surveillance conducted under § 702 of the FISA Amendments Act of 2008 ("FAA").¹ Section 702, codified at 50 U.S.C. § 1881a, establishes procedures for the warrantless surveillance of targeted persons overseas "to acquire foreign intelligence information." Because communications to and from a target under § 702 are swept up without reference to who is sending them and without any determination of probable cause, the FAA results in the "incidental" interception, collection, and retention of communications from unconsenting U.S. persons including, in this case, Mr. Muhtorov.

Judicial review of § 702 authorizations is narrow, and until the Snowden leaks in 2013, the American public was led to believe that the government did not query or use FAA-acquired surveillance against non-targeted U.S. persons. *See Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138 (2013). The belated notice in this case was part of the Snowden fallout and the revelation, post-*Clapper*, that the Executive Branch does, in fact, use FAA-acquired information to investigate U.S. persons for suspected criminal activity, and that it intends to use it against Mr. Muhtorov here.

¹ The FAA added Title VII to the FISA statute, which establishes "Additional [intelligence gathering] Procedures Regarding Certain Persons Outside the United States." It is intended to sunset on December 31, 2017. *See* P.L. 110-261, § 403(b)(1), 122 Stat. 2474, as amended, appearing in 50 U.S.C. § 1881 note.

In his renewed Motion, Mr. Muhtorov moves to suppress all of the FAA-acquired evidence in this case and the “fruits thereof” on grounds that § 702's authorization and implementation procedures permit the government to collect and retain the communications of U.S. persons without a warrant and without probable cause in violation of the Fourth Amendment. Alternatively, as an “aggrieved person” entitled to challenge the lawfulness of the acquisitions directly under § 702, he argues the statute was unlawfully applied to him and seeks discovery into the means and methods of the government’s FAA surveillance in this case to substantiate that claim. With the entry of the ACLU as co-counsel for the defense, briefing has emphasized the former, with Mr. Muhtorov serving as the *Clapper*-qualified² successor to the plaintiffs in that case, who were deemed insufficiently “harmed” by § 702's surveillance procedures to have standing to pursue a Fourth Amendment challenge. I find the *Clapper* argument attenuated by Mr. Muhtorov’s status as a criminal defendant – rather than an incidental interceptee generally – and that his privacy-related *Clapper* claim is transformed by that fact. As a U.S. person and a criminal defendant, Mr. Muhtorov is entitled to the full panoply of statutory and constitutional protections afforded under § 702 and the U.S. Constitution. As a criminal defendant whose communications were captured pursuant to FISA Title I and III

² In *Clapper v. Amnesty Int’l USA*, __ U.S. __, 133 S. Ct. 1138 (2013), Justice Alito writing for a majority of the Supreme Court held that attorneys, human rights, and media organizations lacked article III standing to challenge the constitutionality of § 702 because they could only speculate that their communications had been or would be incidentally acquired during FAA surveillance of their clients or other targeted persons abroad. With the government’s notice in this case, the acquisition of Mr. Muhtorov’s communications is demonstrable and he is therefore “*Clapper*-qualified” to challenge the law.

surveillance targeting an agent of a foreign power, however, these protections are counteracted to a significant extent by FISA and prerogatives long recognized in U.S. law regarding the Executive's primacy in the arena of foreign affairs and national security.

My concern as a trial court judge is with the individual criminal defendants before me and their rights to due process and a fair trial. The constitutional question at issue is one the Executive and courts have wrestled with since the Supreme Court's acknowledgment in the 1972 *Keith*³ case of the dilemma invited when warrantless national security intelligence surveillance uncovers evidence of crime. The question here is where – on the continuum between the largely unfettered authority the government enjoys in national security matters and foreign intelligence surveillance on the one hand, and its constitutionally limited authority to investigate its citizens for crimes – stands Mr. Muhtorov.⁴ It is a particularized inquiry of the most solemn kind. While I am convinced the FAA is susceptible to unconstitutional application as an end-run around the Wiretap Act and the Fourth Amendment's prohibition against warrantless or unreasonable

³ *United States v. United States Dist. Court for the Eastern Dist. of Mich.*, 407 U.S. 297 (1972)(known as the *Keith* case).

⁴ I note Mr. Jumaev has filed his own renewed Motion to Suppress and/or for Discovery (Doc. 521), insisting that FAA must have informed the government's investigation and indictment of him notwithstanding the government's disclaimer and the fact that it filed no Notice of Intent to Use FAA-Acquired information against him in this case. Based on the government's representations that it does not intend to use FAA-acquired evidence against him and my *ex parte* review of all of the classified information in this case, I conclude Mr. Jumaev is not an "aggrieved person" authorized under 50 U.S.C. § 1806(e) to move to suppress such evidence or to bring an as-applied constitutional challenge to Section 702. The question of whether the disclaimer deprives Mr. Jumaev of standing to assert a facial challenge to the FAA under *Clapper* is an open one, in my view, but one, given my ruling in this case, that does not need to be answered. I limit my analysis in this opinion to the constitutional arguments raised by Mr. Muhtorov.

searches, I am equally convinced that it was not unconstitutionally applied to Mr. Muhtorov. Based on my *in camera* review of the classified and unclassified documents made available to me, the FAA surveillance at issue was narrowly tailored to the government's foreign intelligence-gathering prerogatives. Because I find Section 702 to have been constitutionally applied in this case, the facial challenge to the FAA must be denied. I will address Mr. Muhtorov's request for specific, additional discovery and declassification in a separate order, after conducting one or more prefatory CIPA § 4 hearings on the subject.⁵

I.

BACKGROUND AND PROCEDURAL HISTORY.

Jamshid Muhtorov was born in Jizzak, Uzbekistan, when that country was still under communist rule. He is the oldest of five children. After graduating from a technical university, Mr. Muhtorov was offered a position with the Ezgulik Human Rights Society in Uzbekistan, becoming the head of the Jizzak branch in 2003.

During the course of his work with Human Rights Watch, foreign embassies and NGOs, Muhtorov came under the increasing scrutiny of Islam Karimov, the last president

⁵ Section 4 of the Classified Information Procedures Act (CIPA) provides that “[t]he court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.” I have, to date, accepted the government's averred classification assertions as offered. Through the upcoming § 4 process, I intend to put the government through its paces to justify them, and to urge the declassification that was promised for much of the Muhtorov and Jumaev-related discovery in this case.

of Soviet Uzbekistan who became and remains the first president of independent Uzbekistan. This scrutiny intensified in May 2005, and in 2006, according to Human Rights Watch, Mr. Muhtorov was himself threatened and beaten. With the help of other activists, Mr. Muhtorov fled to Kyrgystan, and then, with his wife and children to the United States.

Mr. Muhtorov and his family were admitted to the United States as political refugees in February 2007. They settled in Colorado. Mr. Muhtorov has no criminal record and, until his arrest in January of 2012, had never been arrested. He is a legal permanent resident of the United States.⁶

The operative Second Superseding Indictment (Doc. 59) charges Mr. Muhtorov with two counts of providing and attempting to provide material support and resources to the Islamic Jihad Union (IJU), and Muhtorov and Jumaev with one count of conspiring to commit that offense, in violation of 18 U.S.C. § 2339B. If convicted, each faces a maximum term of imprisonment of 15 years.

The allegations in the indictment were initially attributed to information gleaned in investigations of Mr. Muhtorov's computer, email accounts, private residence, and personal effects. *See* Criminal Compl. (Doc. 1)(and attached Affid. of FBI Special Agent Hale). When the government formally notified Mr. Muhtorov that it intended to use FISA-acquired information against him in the proceedings (Doc. 12), Mr. Muhtorov

⁶ *See* 50 U.S.C. § 1801(i)(defining “United States person” as, among other things, “a citizen of the United States” or “an alien lawfully admitted for permanent residence”).

exercised his right as an “aggrieved person” under the statute and moved to suppress. (Docs. 14, 125). I denied that Motion in a written Order issued September 24, 2012 (Doc. 196), applying the standards set forth at 50 U.S.C. § 1806(e) & (f) and finding the surveillance and physical searches at issue were lawfully authorized and conducted. I specifically concluded that the attested facts submitted to the FISA Court supported a finding of probable cause to believe the target was an “agent[] of a foreign power,” and concluded that the FISA application and related materials should not, in the interest of national security, be disclosed. *Id.* p. 3. I denied Mr. Jumaev’s related Motion on the same basis.

On October 25, 2013, the government filed a Second Notice of Intent to Use FISA-acquired Information (Doc. 457), formally notifying Mr. Muhtorov of its intent to use information obtained or derived from the acquisition of foreign intelligence information under the Foreign Intelligence Surveillance Act of 1978, “as amended,” and citing 50 U.S.C. § 1881a. Given its timing in the Snowden-*Clapper* aftermath, the Notice was clearly intended to notify Mr. Muhtorov that he was a member of the previously undisclosed class of U.S. persons whose international communications had been monitored and acquired incidently to surveillance conducted under § 702 of the FAA. Viewing the affidavit informing the publicly available Complaint in this case in that light, it is clear that FAA surveillance overseas resulted in the acquisition of communications later traced to Muhtorov. *See* Affid. of FBI Agent Hale (attached as Ex. A to Complaint (Doc. 1)). What was acquired and over what period of time is classified information that

has not yet been shared with the defense.

Foreign Intelligence Gathering and FISA.

Presidents since FDR have claimed an inherent constitutional authority to conduct electronic surveillance in national security matters without prior judicial approval. The authority is grounded in Article II of the Constitution, which charges the Executive to “preserve, protect and defend the Constitution of the United States.” This authority was accorded great deference for many years, until that began to change in the early 1970s.⁷

In 1972, the Supreme Court took up the question in *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), a case involving the bombing of a CIA building and the warrantless surveillance that led to the indictment of the U.S. persons involved. Justice Powell, writing for the majority, rejected the government’s assertion of a blanket national security exception to the Fourth Amendment’s warrant requirement as codified in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the “Wiretap Act”), concluding the government’s concerns did not justify a departure from the customary Fourth Amendment requirement of judicial pre-approval under the circumstances presented.⁸ *Id.* at 323-24. The Court expressly refused, however, to “judge[] the scope of the President’s surveillance power with respect to the activities of

⁷ See Fiss, O., “Even in a Time of Terror,” 31 Yale Law & Policy Rev. 1 (2012).

⁸ Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the “Wiretap Act”) governs domestic electronic surveillance activities and requires federal, state, and other officials to obtain judicial approval on a specific showing of probable cause before intercepting “wire, oral, and electronic” communications such as telephone conversations and e-mails.

foreign powers, within or without [the U.S.],” *id.* at 308, leaving that question open. The Court further recognized potential distinctions between national security surveillance and “surveillance of ‘ordinary crime,’” and invited Congress to consider protective standards for the former different from those prescribed in Title III that took these distinctions into account. *Id.* at 322-23. “Different standards,” the Court acknowledged, “may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.” *Id.* at 323.

The Watergate scandal in 1974 thrust the Executive’s use of electronic surveillance into the public eye. Revelations during several Senate Committee hearings revealed a host of warrantless privacy infringements of U.S. citizens in the name of national security, including wiretapping of congressional staffers, anti-war protesters, and civil rights activists including Dr. Martin Luther King. After fourteen Senate Reports and significant debate, Congress enacted the Foreign Intelligence Surveillance Act “to regulate the use of electronic surveillance within the United States for foreign intelligence purposes.” *See* S. Rep. 95-604, p. 7 (1977). President Carter signed it shortly thereafter. 92 Stat. 1783, 50 U.S.C. § 1801 *et seq.*

In constructing a framework for foreign intelligence surveillance that balanced the Executive’s foreign intelligence and security prerogatives with Americans’ privacy interests, Congress defined “electronic surveillance” narrowly to include only foreign

intelligence collection activities that impacted U.S. persons or took place on U.S. soil,⁹ and prohibited anyone from engaging in “electronic surveillance under color of law *except* as authorized by this Act.” 50 U.S.C. § 1809(a)(emphasis mine). Congress then created two specialized foreign intelligence courts – the FISA Court (FISC) and the FISA Court of Review (FISR) – that would approve and review the approval of “electronic surveillance” under the Act. 50 U.S.C. § 1803(a) & (b), *discussed* in *Clapper*, 133 S. Ct. at 1143. Surveillance authorization would be given if there was “probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power”; and if minimization procedures are in place that meet with FISC approval under the standards articulated in the statute. *See* 50 U.S.C. § 1805(a). As will be

⁹ *See* 50 U.S.C. § 1801(f)(1)-(4)(§ 1801(f)(1)-(4)(defining “electronic surveillance” in terms of wire or radio communications targeting a person “in,” acquired “in,” or intended for or received by someone “in,” the “United States”). Given that international communications in 1978 were carried through satellite signals or over transoceanic cables subject to interception offshore, Congress understood this language would exempt NSA’s foreign-to-foreign as well as most of its international communications surveillance from regulation, because neither would fall within the definition of “electronic surveillance” under the Act:

“The language of this amendment exempts . . . foreign intelligence gathering . . . if the acquisition does not come within the definition of ‘electronic surveillance’. . . . Specifically this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.”

See United States v. Mohamud, Crim., Case No. 10-cr-475-KI, *slip op.* at p. 12, 2014 WL 2866749 (D. Or. June 24, 2014)(quoting S. Rep. No. 95-701, at 71 (1978)).

discussed in more detail below, “minimization procedures” serve as the principle means of protecting the Fourth Amendment privacy interests of U.S. persons whose communications are caught up in foreign intelligence surveillance under FISA.¹⁰

Expansion of FISA Authority.

Almost as soon as it was enacted, pressure began to build to clarify and expand the Executive’s foreign surveillance authority under the FISA statute. Increasing terrorist activity raised the stakes¹¹ and changes in communications technology brought intelligence surveillance intended to remain outside FISA’s purview within its definition of domestic surveillance and thus subject to FISA Court review and regulation.¹²

In 1981, President Reagan issued Executive Order 12333, reaffirming the Executive’s inherent authority to conduct covert operations and collect information on

¹⁰ “Minimization procedures” under FISA are defined as “specific procedures . . . adopted by the Attorney General, that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” 50 U.S.C. § 1801(h).

¹¹ The 1979 seizure of the U.S. embassy in Tehran; a series of Libyan and Hezbollah bombings, attacks and hostage taking beginning in 1982 and continuing throughout the 80s and early 90s, including the 1988 bombing of a Pan-Am flight over Lockerbie, Scotland, in 1988; the 1993 World Trade Center bombing in New York; and the Oklahoma City bombing in 1995 are but a few examples.

¹² The advent of the internet, for example, meant that foreign communications previously transmitted via satellite or transoceanic cables in 1978 were now carried over fiber optic cables. Because these cables were arguably “wires,” foreign surveillance that would have been excluded from FISA regulation in 1978 was rendered potentially unlawful due merely to a change in technology, rather than any intentional decision by Congress. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Sel. Comm. on Intel.*, 110th Cong., 1st Sess. (2007) at pp. 9-19 (testimony of the Director of National Intelligence).

“foreign powers, organizations, persons, and their agents” without reference to FISA, and specifically authorizing “elements of the intelligence community . . . to collect retain, or disseminate information concerning United States persons.” EO 12333, Parts 2.2, 2.3.¹³ In 1995 and 1998, Congress amended FISA directly, first to include physical searches, 50 U.S.C. §§ 1821-29, and then the installation and use of pen register and trap and trace devices, §§ 1841-46, “for foreign intelligence purposes.”

Then in 2001, foreign terrorists carried out the coordinated 9/11 attacks on New York City and the Pentagon, killing nearly 3,000 people on American soil. Within weeks, both President George W. Bush and Congress had acted to expand Executive surveillance authority and facilitate more effective coordination between the intelligence community and federal law enforcement agencies. In October 2001, Congress passed the USA PATRIOT ACT,¹⁴ sweeping legislation that modified multiple existing laws and enhanced the government’s law enforcement authority as it related to investigating and prosecuting terrorism.¹⁵ Among other things, the PATRIOT ACT revised FISA § 104's

¹³ EO 12333's complete text appears at 46 Fed. Reg. 59941, 3 C.F.R.

¹⁴ United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the “USA PATRIOT ACT”), Pub. L. 107-56 (October 26, 2001).

¹⁵ The USA PATRIOT Act not only amended FISA, but also the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Pen Register and Trap and Trace Statute, Money Laundering Act, Immigration and Nationality Act, Money Laundering Control Act, Bank Secrecy Act, Right to Financial Privacy Act, and the Fair Credit Reporting Act all were impacted by USA PATRIOT Act amendments. *See generally*, Congressional Research Service (2002b), “The USA PATRIOT Act: A sketch.” [On-line]. Available: <http://www.fas.org/irp/crs/RS21203.pdf>

“purpose” requirement. Responding to a series of court cases and intelligence agency policies that had erected a “Wall” between foreign intelligence and criminal investigations, the ACT authorizing FISA applications on a certification that foreign intelligence gathering was a “significant,” rather than “primary” purpose of the surveillance sought. *Compare* 50 U.S.C. § 1804(a)(6)(B) (2008) *with* 50 U.S.C. § 1804(a)(7)(B) (2000)(change discussed at length in *United States v. Abu-Jihaad*, 630 F.3d 102, 122-23 (2d Cir. 2010)). President Bush, meanwhile, responded to the 9/11 attacks by authorizing the NSA to conduct warrantless wiretapping of telephone and e-mail communications in the United States outside the purview of FISC entirely, as long as one party to a communication was located outside the United States and a participant in “the call was reasonably believed to be a member or agent of Qaeda or an affiliated terrorist organization.” *See Clapper*, 133 S. Ct. at 1143-44. Until 2005, neither the public nor most members of Congress were aware the President’s Terrorist Surveillance Program (TSP) existed.

President Bush’s confirmation in December 2005 that the NSA had been conducting warrantless electronic surveillance of U.S. persons without even FISA Court approval prompted Congress, once again, to conduct a “vigorous inquiry” into the Executive’s secret surveillance activities. *See* S. Rep. No. 110-209, 1st Sess. 1 (2007). With all parties in agreement that FISA required updating, Congress set to work. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the H.*

Permanent Select Comm. on Intel., 109th Cong., 2d Sess. (2006).¹⁶

The PAA and Elimination of the “Foreign Agent” Probable Cause Requirement

As a result of these efforts, Congress enacted the Protect America Act (“PAA”) in August 2007, a temporary measure that brought the Executive’s TSP authority into the FISA fold. Codified at 50 U.S.C. § 1805a, b & c, the PAA permitted the Director of National Intelligence and the Attorney General to authorize the acquisition of foreign intelligence information “concerning persons reasonably believed to be located outside the United State” without reference to their status as foreign agents, limited solely by the establishment of targeting and minimization procedures to “preserve the privacy interests

¹⁶ During hearings, Congress heard testimony on the ways the advancement of communications technology since 1978 had created unforeseen consequences under FISA. Transmission over an integrated global communications grid blurred the distinction between domestic and offshore acquisition. Domestic communications between neighbors in Peoria could travel around the world and be intercepted abroad. Foreign-to-foreign communications that were previously beyond FISA’s reach could be intercepted in the United States.

[As a communication travels the global network,] NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science . . . Intercept of a particular communication . . . is always probabilistic, not deterministic [and] [n]o coverage is guaranteed.

FISA for the 21st Century: Hg. before the S. Comm. on the Judiciary, 109th Cong., 2d Sess. (2006)(statement of NSA Director General Michael V. Hayden). The necessary fix, Congress was told, was a “technology-neutral” framework for surveillance of foreign targets – focused not on “how a communication travels or where it is intercepted,” but on “who is the subject of the surveillance, which really is the critical issue for civil liberties purposes.” *FISA Modernization Hg.* at 46 (statement of Asst. Atty Gen. Kenneth L. Wainstein). With these changes, it was implied, the original balance between strictly “foreign” foreign intelligence gathering and foreign intelligence gathering that impacted Americans struck by FISA in 1978 could be reconstituted, and secret programs like TSP could be brought to light and integrated into the FISA framework.

of persons in the United States.” S. Rep. No. 209, 110th Cong. 1st Sess. at 5-6. The PAA was revised and incorporated into FISA by the FISA Amendments Act of 2008, becoming § 702 of a new FISATitle VII.

Section 702, like the PAA before it, authorizes the Attorney General and the Director of National Intelligence to authorize jointly, “for a period of up to 1 year,” the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. § 1881a(a). Like the PAA, § 702 permits the government to intercept all communications to and from the target, including those of U.S. persons, without demonstrating probable cause that either is a foreign power or the agent of a foreign power, and without identifying the facilities or places where the electronic surveillance will occur. FAA procedure simply requires the Attorney General, in consultation with the Director of National Intelligence, to select a target and adopt guidelines the Attorney General certifies will “ensure” compliance with appropriate targeting and minimization procedures, as well as the limitations on § 702 surveillance authority set forth in § 1881a(b). *See* § 1881a(f)&(g). If the FISC finds the AG’s certifications, targeting, and minimization procedures are “consistent with [the FAA’s requirements] and with the fourth amendment to the Constitution of the United States,” it “shall” enter an order approving the certification and use of the procedures for the acquisition. 50 U.S.C. § 1881a(i).

Section 702's limitations are significant, but largely conclusory and “riddled with loopholes.” An acquisition under § 702(a) may not “intentionally” target a person

“known” at the time of acquisition to be located in the United States (§ 1881a(b)(1)), or “intentionally target” a person “reasonably believed to be located outside the United States” if the “purpose” of such acquisition is to target a “particular, known person reasonably believed to be in the United States.” § 1881a(b)(2). Also, acquisitions must be “conducted in a manner consistent with the fourth amendment to the Constitution.” § 1881a(b)(5). But the government is the sole arbiter of its “knowledge,” “intent,” “purposes,” and “conduct.”¹⁷ The government can continue “incidentally” acquiring a person’s communications under § 702 even after such reveals evidence of a crime, as long as the government avoids learning that the person is a U.S. person or located in the United States. It can avoid seeking Title I or Title III authority to target the person directly by simply declining to call that person a “target.” It can say it is “conducting” this surveillance consistently with the fourth amendment, but § 702 provides no mechanism for FISC to assess whether that is the case. For an excellent discussion of the FAA’s weaknesses and prescriptions for remedying them, *see* T. Anderson, “Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act,” 8 Harv. Law & Policy Rev. 413 (Summer 2014).

¹⁷ Compliance with § 702(b) limitations and with the Attorney General’s proffered targeting and minimization procedures is self-monitored and self-executing under the FAA, as judicial review is limited to the initial authorization and any reauthorizations sought by amendment. *See* § 1881a(i). The FAA requires that the Attorney General and Director of National Intelligence conduct a “semi-annual assessment” of compliance with the targeting and minimization procedures of a particular surveillance authorization, § 1881a(l), but other than submitting that assessment to FISC and to congressional intelligence and judiciary committees, the FAA requires no action on the assessment and no judicial review on the part of FISC.

FISA and Law Enforcement.

Our concern in this case, of course, is the confluence of FISA and law enforcement, i.e., what happens when FISA surveillance results in the acquisition of evidence of a crime. It is clear that FISA surveillance is more than simply foreign intelligence gathering, and that its purpose since its inception has been the discovery and investigation of foreign intelligence crimes. *See In re Sealed Case*, 310 F.3d 717, 725 (Foreign Int. Surv. Ct. Rev. 2002). U.S. persons may be authorized targets, and surveillance may be part of an investigative process designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of foreign powers. *Id.* (quoting S. Rep. No. 95-701, at 10-11 (1978)). The question has always been where these two functions merge, i.e., where FISA-acquired electronic surveillance information, which is acquired *without* a warrant under the Wiretap Act, is used against an U.S. person who would otherwise enjoy the protections of that Act.

Before the enactment of the FAA, case law developed permitting the use of FISA-acquired evidence against U.S. persons in criminal prosecutions as long as there was probable cause to believe those persons were “foreign powers” or “agents of a foreign power” (50 U.S.C. § 1805(a)(2)) and the surveillance was properly conducted “to acquire foreign intelligence information.” 50 U.S.C. § 1802(a)(1). *E.g. United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1988)(as long as the purpose of FISA surveillance is foreign intelligence gathering, that purpose is not

changed merely because government anticipates using fruits of FISA surveillance in criminal prosecution). The purpose of the surveillance cannot be a ruse. *See United States v. Johnson*, 952 F.2d 656, 572 (1st Cir. 1991), *cert. denied*, 506 U.S. 816 (1992)(government cannot use FISA as an “end-run around the Fourth Amendment’s prohibition of warrantless searches” by drumming up a foreign intelligence purpose for ordinary criminal investigation); *United States v. Troung Dinh Hung*, 629 F.2d 908, 916 (4th Cir. 1980)(targets must “receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution.”) But unless surveillance is conducted “solely” for law enforcement purposes, the Fourth Amendment under *Keith* is flexible enough to justify the use of FISA-acquired evidence in criminal prosecutions even without a Title III warrant. *See U.S. v. Duka*, 671 F.3d 329, 345 (3d Cir. 2011)(evidence derived from a reasonable search is admissible in a criminal trial); *Abu-Jihaad*, 630 F.3d at 12 (Fourth Amendment does not require the government to identify a primary purpose or limit its ability to secure a warrant to satisfaction of the standards for that purpose; rather, the government may secure a warrant under the probable cause standards applicable to any purpose that it pursues in good faith).

Under the FAA, § 702 does away with the § 105's probable cause requirement, permitting the government to target persons based solely on their physical presence outside the United States, and to intercept communications to and from those persons, as long as the surveillance was conducted “to acquire foreign intelligence information.” § 1881a(a). Mr. Muhtorov contends this change distinguishes the case law allowing the

use of FISA-acquired evidence in criminal prosecutions, and renders the use of FAA-acquisitions against U.S. persons in criminal prosecutions unconstitutional.

II.

DISCUSSION.

Mr. Muhtorov contends the fruits of the government's § 702 surveillance must be suppressed because the statute that authorized the surveillance is unconstitutional. He argues the FAA violates the Fourth Amendment by authorizing surveillance that contravenes the warrant clause and, independently, surveillance that is unreasonable. He also argues the FAA violates Article III by requiring judges to issue advisory opinions in the absence of a case or controversy, citing my opinion in *United States v. Smith*¹⁸ in support.

The FAA and Article III's Case or Controversy Requirement

I pause briefly to address Mr. Muhtorov's assertion that the FAA is unconstitutional because it violates Article III's "case or controversy" requirement. His argument is novel and elegant, but I will not be the first to adopt it. Plainly stated, Muhtorov argues the FAA assigns to the FISA Court a role "fundamentally incompatible with the case-or-controversy requirement" because it compels FISC to "evaluate in a vacuum whether proposed targeting and minimization procedures comply with the statute

¹⁸ *United States v. Smith*, 686 F. Supp. 847 (D. Colo. 1988)(declaring Sentencing Reform Act of 1986 unconstitutional, in part, because role played by Article III judges on Sentencing Commission violated principles of separation of powers).

and the Constitution” without any particularized facts or context. Mot. (Doc. 520) at 45.

The authority he cites for his proposition, however, is either inapposite,¹⁹ or distinguishable,²⁰ and none applies the concept in the context of the “neutral magistrate” or other arbiter of search authorizations or warrants under the Fourth Amendment.

Mr. Muhtorov’s strongest argument is that courts that have rejected Article III challenges to the *traditional* FISA process have done so because the FISC’s job is a particularized one – i.e. that under 50 U.S.C. § 1805(a) and (b), FISC considers concrete facts about a specific person to be monitored and the facilities to be targeted. *Citing U.S.*

¹⁹ *Flast v. Cohen*, 392 U.S. 83, 97 (1968)(addressing case in controversy requirement in context of standing analysis for taxpayer suit challenging validity of federal spending on textbooks); *Citizens Concerned for Separation of Church & State v. City & Cnty. of Denver*, 628 F.2d 1289, 1295 (10th Cir. 1980)(using case or controversy requirement as source for standing analysis, finding citizens lacked standing to bring First Amendment challenge to City’s creche display because there was no showing of causal connection between the creche display and any injury in fact to plaintiff); *In re Summers*, 325 U.S. 227, 241 (1937)(holding that a claim of a present right to admission to state bar association and denial of that right is a case or controversy that may be reviewed under Article III when federal questions are raised). The citation to my opinion in *Smith* is more interesting, because although my ruling there passed on a completely different aspect of the separation of powers doctrine, I observed that article III judges “[d]ischarging tasks other than the deciding of cases and controversies” would involve them in the process of policy and thereby “weaken confidence in the disinterestedness of their judicatory functions.” 686 F. Supp. at 855 (quoting *In re Sealed Cases*, 838 F.2d 476, 512 (D.C. Cir. 1988)). The point is correct, in my view, but not particularly germane. If the concern is that FISC’s participation in § 702 authorizations undermines the perceived impartiality or detachment of the judiciary from law enforcement, it is of a kind with concerns over judges participation in secret or *ex parte* proceedings of all types, and wiretap authorizations generally.

²⁰ *See New York v. Ferber*, 458 U.S. 747, 768 (1982)(addressing the need to focus on “flesh-and-blood” applications of fact to law in context of First Amendment overbreadth challenge to child pornography statute); *Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 239 (1937)(construing Declaratory Judgment Act’s “actual controversy” requirement in context of Article III’s limitation of judicial power to “‘cases’ and ‘controversies,’” holding the term “‘controversies,’ if distinguishable at all from ‘cases,’ is so in that it is less comprehensive than the latter, and includes only suits of a civil nature”).

v. Megahey, 553 F. Supp. 1180, 1186 (E.D.N.Y. 1982), *aff'd* 729 F.2d 1444 (2d Cir. 1983), and *aff'd on other grounds sub nom. United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984). In *Megahey*, defendants argued that FISC was not constitutionally authorized under Article III because FISA required it to issue orders on an *ex parte* basis without any adversarial proceedings. The district court rejected the argument, stating

Applications for electronic surveillance submitted to FISC pursuant to FISA involve concrete questions respecting the application of the Act and are in a form such that a judge is capable of acting on them, much as he might otherwise act on an *ex parte* application for a warrant. In the case of each application, the FISC judge is statutorily obliged to ensure that each statutory prerequisite is met by the application before he may enter a surveillance order. The FISC judge who is faced with a surveillance application is not faced with an abstract issue of law or called upon to issue an advisory opinion, but is, instead, called upon to ensure that the individuals who are targeted do not have their privacy interests invaded, except in compliance with the detailed requirements of the statute.

553 F. Supp. 1180 at 1197.

That the FAA altered this analysis is undeniable. The “concrete questions” and “individual targets” contemplated by traditional FISA authorization requests have been excused in authorization requests under the FAA. Moreover, the “incidental interceptees” with whom we are concerned are nameless, faceless, and transient in the context of § 702 surveillance, and their privacy interests are evaluated solely in the context of the certified targeting and minimization procedures FISC is asked to approve.

The government dismisses this distinction, arguing FAA authorization approval is more similar to traditional FISA approval than different, and constitutionally not unlike other statutory schemes in which courts assess the reasonableness of standards and

procedures for conducting searches or surveillance consistently with Article III. Govt's Unclassified Resp. to Mot. Suppress (Doc. 559) at 79-80 (citing *United States v. Tortorello*, 480 F.2d 764, 772-73 (2d Cir. 1973)(analyzing adequacy of New York statutory procedures for reauthorizing surveillance after original authorization accidentally uncovered evidence of crime) and *Camara v. Municipal Court*, 387 U.S. 523, 537-38 (1967)(approving warrantless inspection provision of municipal housing code – standard may be based on passage of time or nature of the building, and not necessarily specific knowledge of particular dwelling)). Accordingly to the government, FISC's job of analyzing the reasonableness of electronic surveillance by weighing national security interests against the privacy interests of potential subjects is a "traditional judicial function," citing *Halperin v. Kissinger*, 606 F.2d 1192, 1201 n.59 (D.C. Cir. 1979), and is not rendered otherwise by the fact that the potential subjects are not identified with particularity.

I do not dismiss the distinction so easily. FISC's job under the FAA is substantively different than it is under traditional FISA and under any of the other examples of "traditional judicial function" the government cites. Under the FAA, incidental interceptees are part of the surveillance contemplated, but no particularized information about them or their communications practices is presented to FISC for consideration. Each of the scenarios cited by the government is different: There would have been no "case or controversy" in *Tortorello* without Arthur Tortorello, and no "case or controversy" in *Camara* without Roland Camara.

FISC's role in approving the surveillance of individual foreign powers or agents under traditional FISA is qualitatively different from its role in approving the surveillance and incidental acquisition of strangers' communications under the FAA. Whether that role offends Article III sufficiently to invalidate § 702 as a tool for gathering foreign intelligence information is one I leave to a higher court.²¹ For purposes of the case before me, my judgment is that it does not.

The FAA's Validity Under the Fourth Amendment.

While FISA authorizes the government to conduct relatively narrow surveillance of individuals reasonably believed to be "foreign agents" or "foreign powers," the FAA permits the government to monitor any person, and that person's contacts, without reference to his foreign status or agency. By permitting the government to acquire "essentially any communication that originates or terminates outside the United States,"

²¹ I note that during the course of briefing in this case, Judge King in the District of Oregon issued his opinion in *United States v. Mohamud*, 2014 WL 2866749 (2014), upholding the FAA and the government's disclosure that it had used FAA-acquired evidence to secure the conviction of a U.S. person. Defendant's arguments in *Mohamud*, discussed further *infra*, included an Article III challenge similar to Mr. Muhtorov's here. While I agree with several of Judge King's legal conclusions in *Mohamud*, I find his analysis of defendant's "case or controversy" arguments unpersuasive. Judge King spent most of his discussion couching defendant's arguments in terms of a separation of powers challenge, which he contends has been put to rest by *Mistretta v. United States*, 488 U.S. 361 (1989). *Id.* at *10-11. As set forth in n. 19, *supra*, I find the separation of powers analysis inapposite to the "case or controversy" argument raised. Judge King's further discussion equates FISC's role in FAA surveillance authorizations to the "neutral and detached" review conducted by magistrates under the Wiretap Act, citing *Keith*. *Id.* at *11. In so doing, Judge King did not address the fundamental differences between wiretap authorization reviews conducted in criminal cases and traditional FISA on the one hand, and the FAA on the other. As a result, I do not believe *Mohamud* moves the ball forward on this issue.

Mr. Muhtorov contends the FAA violates both the Fourth Amendment's warrant clause and its ban on unreasonable searches and seizures. Mot. Suppress (Doc. 520) at 21.

The Fourth Amendment's Warrant Requirement

The Fourth Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the places to be searched, and the persons or things to be seized.

The modern Supreme Court has done away with an interpretation of the Fourth Amendment that requires a warrant, a probable cause determination, “[or, indeed, any measure of individualized suspicion,” in every circumstance, before a search may be lawful. *Mohamud*, 2014 WL 2866749 at *12 (quoting *Nat’l Treasury Emp. Union v. Von Raab*, 489 U.S. 656, 665 (1989)(holding suspicionless drug-testing of certain United States Custom Service employees not unreasonable under the Fourth Amendment)). The warrant requirement does not apply to activities of the United States directed against aliens in a foreign territory, *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990)(search of the Mexican residences of a Mexican citizen), and does not apply to even U.S. persons if the government establishes a defensible “special need” to dispense with it. *See e.g. Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)(exception to Fourth Amendment's warrant requirement “when special needs, beyond the normal need for law enforcement, makes the warrant and probable-cause requirement impracticable.”)).

Courts have combined these concepts to carve out a “foreign intelligence

exception” to the warrant requirement,²² which Mr. Muhtorov urges me to reject.²³ I find the special need/foreign intelligence exception argument somewhat academic and limiting, because the standard ultimately is one of reasonableness, and it is on that standard that the constitutionality of § 702's warrantless surveillance authorization must be decided. *See Samson v. California*, 547 U.S. 843, 852 n.3 (2006)(declining to address whether California's parole search condition was justified “special need” under *Griffin* because determination that condition was reasonable rendered examination unnecessary).

On its face, § 702 surveillance targets individuals *outside* the United States “to acquire foreign intelligence information.” The reasonableness of that targeting, without a warrant, is not the essence of our inquiry. *See In re Directives* [redacted text] *Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (For. Intel. Surv. Ct. Rev. 2008)(Even if a foreign intelligence exception applies in a given case, “governmental action intruding on the individual privacy interest [of U.S. persons] must comport with the Fourth Amendment's reasonableness requirement.”). Our concern is with the axiomatic corollary of that targeting, *i.e.*, that U.S. persons' communications with the target are *perforce* acquired as part of that targeted surveillance, and may be used

²² *See Duka*, 671 F.3d at 341 (stating “courts have concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of ‘foreign intelligence exception’ to the Fourth Amendment's warrant requirement,” and collecting cases).

²³ Mot. Suppress (Doc. 520, at 27, 30)(there is no “special needs” exception to the warrant requirement for foreign intelligence and “not basis to conclude” the requirement is unworkable here).

against them in criminal investigations on American soil without any reasonable suspicion or probable cause determination having been made as to *them*.

Reasonableness.

The touchstone of constitutionality under the Fourth Amendment is reasonableness. It is a fluctuating rather than fixed standard. It depends not only on an analysis of the discrete facts incident to a finding of probable cause (and, for that matter, the search and/or seizure itself), but also the intent and purpose of the established laws of the United States. Because the test is one of reasonableness, the panoply of relevant factors must be considered. In the instant case, the charges against Mr. Muhtorov are premised in the constitutional requirement that the Executive has broad powers to protect the United States against foreign threats. What may be unreasonable in a purely domestic matter may, on balance, be considered reasonable in the context of the security of the nation in dealing with foreign powers and organizations that pose a threat. “It must be remembered that what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.” *Elkins v. Unites States*, 364 U.S. 206, 222 (1960).

To analyze whether a government search is reasonable under the Fourth Amendment, the court examines the totality of the circumstances. *Samson v. California*, 547 U.S. 843, 848 (2006). The court weighs “the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual’s privacy.” *Maryland v. King*, ___ U.S. ___, 133 S. Ct. 1958, 1970 (2013)(internal citations and quotations omitted). Under this standard, the modern Supreme Court has approved

statutory schemes requiring arrestees to submit to buccal swab DNA testing solely as a police booking procedure, *see id.*, and parolees to agree in writing to be subject to suspicionless searches at any time, day or night. *Samson*, 547 U.S. at 846 (Thomas, J.)

Mr. Muhtorov argues that in the context of electronic surveillance, reasonableness requires that eavesdropping be “precise and discriminate” and “carefully circumscribed so as to prevent unauthorized invasions of privacy.” Mot. (Doc. 520) at 34 (citing *Berger v. State of New York*, 388 U.S. 41 (1967) and *United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973)). He urges me to look to traditional FISA and Title III as measures of the reasonableness for electronic surveillance, arguing FAA’s approval scheme permitting the generalized acquisition of U.S. persons’ communications without any particularized showing or demonstration of cause is a bridge too far. *Id.* I do not disagree, but find there is more to the balance than that. The fact traditional FISA surveillance requires a particularized demonstration of probable cause and is constitutional does not mean that FAA surveillance is unconstitutional because it does not. The question is the degree of the intrusion, weighed against the government’s legitimate interest in acquiring foreign intelligence information to protect against the commission of serious crimes such as espionage and terrorist acts committed by or on behalf of foreign powers. In my view, the FAA passes the Fourth Amendment test.

Privacy Interest.

As an initial matter, I consider Mr. Muhtorov’s privacy interests. Under § 702, the intrusion on an individual’s privacy is as an incidental third party who is a participant in

intercepted communications with a target overseas. The government contends defendants have little or “severely diminished” expectations of privacy in their communications with non-U.S. persons overseas, *see* Unclassified Br. (Doc. 559) at 59-61, & n. 37, based simply on the fact that those persons could be targets for surveillance both by the U.S. government and by other foreign governments or private interest. While I could never adopt the government’s cynical view of the First and Fourth Amendment, it is true that expectations of privacy are diminished the more information one puts out into the ether, especially the ether of the global telecommunications network.

Fourth Amendment jurisprudence has long recognized a third-party doctrine, i.e., a diminishment or loss of a person’s privacy interests where he reveals information to a third party, even in confidence. *See United States v. Miller*, 425 U.S. 435, 444 (1976)(bank records); *Smith v. Maryland*, 442 U.S. 735 (1979)(use of a pen register by telephone company does not constitute a search within meaning of Fourth Amendment because person has no legitimate expectation of privacy in numbers dialed on his phone). The concept has been held to apply to electronic communications, where “a person’s reasonable expectation of privacy may be diminished in transmissions over the Internet or e-mail that have already arrived at the recipient .” *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). While Mr. Muhtorov and others have a reasonable expectation of privacy in the content of their communications generally, those interests are at least somewhat diminished when transmitted to a third party over the internet.

Weighing Privacy and National Security Interests to Assess Reasonableness.

The intrusion into U.S. persons' legitimate privacy interests under § 702 is less than the generalized "vacuum-cleaner-style mass collection of virtually every person's international communications" of which Mr. Muhtorov, in his role as *Clapper*-qualified antagoniste, complains. Collection must be demonstrably intertwined with the government's efforts to "acquire foreign intelligence information,"²⁴ § 1881a(a), and may not "intentionally target any person known at the time of the acquisition to be located in the United States." § 1881a(b)(1). Approval hinges on findings that "foreign intelligence information" gathering is a "significant purpose" of the surveillance, and limitations against abusing the § 702 surveillance process to effectively target Americans will be observed.

More importantly, as was posited at the beginning of this opinion, *Mr. Muhtorov's* concern is less with the incidental acquisition of his communications by national intelligence agencies during the course of otherwise lawful foreign intelligence gathering, but in the retention and *use* of those communications by federal law enforcement in criminal proceedings against him in a court of law. FISA clearly contemplates that intelligence gathering and law enforcement "tend to merge" in the area of terrorism detection and prevention. *See In re Sealed Case*, 310 F.3d at 725 (citing S. Rep. 95-701

²⁴ "Foreign intelligence information" is defined under FISA as information that "relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . an actual or potential attack . . . sabotage, international terrorism, or the international proliferation of weapons of mass destruction . . . , or clandestine intelligence activities." § 1801(e)(1). It is also information with respect to a foreign power . . . that relates to, and if concerning a United States person is necessary to . . . the national defense or the security of the United States." § 1801(e)(2).

(1978)). The government's interest in using intelligence information to detect and prevent criminal acts of terrorism, and ultimately to punish their perpetrators, is a legitimate governmental interest against which individual FAA privacy intrusions must be weighed.

Relevant to balancing of FAA interceptees' privacy interests against the government's interest in detecting and preventing acts of terrorism, is the fact that the government's *use* of FAA-acquired communications is carefully controlled under FISA. *See id.*, 310 F.3d at 740-41. Minimization procedures must be adopted by the Attorney General for every application under the FAA, *see* § 1881a(e), and must be designed to “minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.” 50 U.S.C. § 1801(h)(1). Procedures must provide for the weeding out of information that is not foreign intelligence information, and the protection of it from dissemination in any manner that identifies a United States person without his consent. § 1801(h)(2). Additional minimization procedures must be established for the retention and dissemination to law enforcement of information that is evidence of a crime, § 1801(h)(3), and provide for how communications to which a United States person is a party may be disclosed, disseminated, or used, and provide time limits for retention. § 1801(h)(4).

Mr. Muhtorov argues that § 702's minimization procedures are inadequate (and the approval scheme therefore constitutionally unreasonable) because they allow the

government to maintain a database of incidently collected information and query it for law enforcement purposes later. These “backdoor searches,” Muhtorov concludes, require a warrant and render the FAA approval scheme unconstitutional. I disagree. Accessing stored records in a database legitimately acquired is not a search in the context of the Fourth Amendment because there is no reasonable expectation of privacy in that information. Evidence obtained legally by one police agency may be shared with similar agencies without the need for obtaining a warrant, even if sought to be used for an entirely different purpose. This principle applies to fingerprint databases and has also been applied in the foreign intelligence context in *Jabara v. Webster*, 691 F.2d 272, 277-79 (6th Cir. 1982).

Applying these standards to the suspicionless incidental acquisition of U.S. persons’ communications contemplated under the FAA, I cannot conclude that the FAA’s approval procedures are per se constitutionally infirm. These acquisitions must be tailored to the very serious purpose of foreign intelligence gathering, as defined in the Act, and may not be used to target U.S. persons as an end-run around Title III. Minimization procedures must weed out acquisitions that are unrelated to foreign intelligence gathering, and inform the retention, querying, and dissemination of those acquisitions for law enforcement purposes in a manner that is consistent with the limitations in § 1881a(b). I note this conclusion is consistent with Judge King’s in *Mohamud* (2014 WL 2866749 at *27), the only other decision to date to have addressed the specific Fourth Amendment challenge to the FAA presented here.

That I do not find the FAA unconstitutional on its face does not *per force* mean that it was constitutionally applied to Mr. Muhtorov. As I have already observed, § 702's authorization procedures are “riddled” with loopholes and there is no judicial oversight of their execution over time. Any acquisition, retention, dissemination, or use of his electronic communications that abused one of these loopholes or exceeded FISC's authorizations in this case would be unlawful. Accordingly, I proceed to consider the constitutionality of the specific § 702 acquisitions of Mr. Muhtorov's electronic communications in this case.

Acquisition of § 702 Materials in this Case.

Other than the specific timeline of the § 702 acquisitions involving Mr. Muhtorov, the relevant facts in this case are straightforward and minimally classified. Nearly all are recited in the Affidavit of Special Agent Hale of the Federal Bureau of Investigation, a public document filed with the court in support of the criminal complaint (Doc.1, filed 01/19/12). The problem with Agent Hale's factual recitation is that it elides any express distinction between the facts gathered as a result of Title I (electronic) and Title III (physical) searches on the one hand, and Title VII (FAA-acquired) information on the other.

The Islamic Jihad Union (IJU) is an extremist organization that splintered from the Islamic Movement of Uzbekistan (IMU) in the early 2000s. The IJU adheres to an anti-Western ideology, opposes secular rule in Uzbekistan, and seeks to replace the current regime with a government based on Islamic law. The IJU first conducted attacks

in April, 2004, targeting a popular bazaar and police at several roadway checkpoints. These attacks killed approximately 47 people, including 33 terrorists, some of whom were suicide bombers. The IJU claimed responsibility for these attacks on multiple militant Islamic websites and denounced the leadership of Uzbekistan. In July, 2004, the IJU conducted simultaneous suicide bombings of the United States and Israeli Embassies in Uzbekistan as well as the Uzbekistani Prosecutor General's Office in Tashkent, Uzbekistan. Claiming responsibility for these attacks, the IJU stated that its martyrdom operations would continue. The IJU also claimed the attacks were committed in support of its Palestinian, Iraqi and Afghan brothers in a global insurgency.

In September, 2007, German authorities arrested three IJU operatives, thus disrupting a plot against unidentified U.S. or Western facilities in Germany. The IJU operatives had available 700 kilograms of hydrogen peroxide and an explosives precursor sufficient in raw material to make the equivalent of about 1200 pounds of TNT. The IJU claimed responsibility for the foiled plot. The IJU has also claimed responsibility for attacks targeting coalition forces in Afghanistan in 2008 including a March suicide attack against a U.S. military post that was allegedly carried out by a German-born Turk.

In April, 2009, Turkish authorities seized weapons and detained extremists with ties to the IJU. The IJU also claimed responsibility for a May 2009 attack in Uzbekistan and numerous attacks in Afghanistan against coalition forces. At all times relevant to the charges against Mr. Muhtorov, the IJU was designated a terrorist organization by the Secretary of State, and has been so designated since June 12, 2005, under the name

Islamic Jihad Group.²⁵

As has already been disclosed, the FISA application at issue in this case was based in part on FAA surveillance and collection. Mr. Muhtorov contends the “incidental” acquisition of his communications and their subsequent retention, querying, and use in criminal proceedings brought against him, was unreasonable under the Fourth Amendment. I have already reviewed the FISA Court’s Title I and Title III approvals and concluded the searches and surveillance conducted under those approvals was lawfully authorized and conducted. I have since performed an exhaustive *in camera* and *ex parte* review of all relevant additional classified materials provided to me by the government, including supplemental classified materials prepared at my request. I conclude on the record before me that a proper and supported application was filed, and that the targeting and minimization procedures forwarded were tailored to the government’s legitimate foreign intelligence purposes and took into account the privacy interests of individuals whose communications would be incidentally acquired. Mr. Muhtorov’s Motion to Suppress Evidence Obtained or Derived under § 702 (Doc. 520) is DENIED. Because I find all legal criteria were met by the government to establish that the searches and surveillance at issue were lawfully authorized and conducted, there is no need to consider the “good faith” alternative basis for denying the Motion to Suppress.

²⁵ Notification of its designation appears at 70 Fed. Reg. 35332-01 (June 17, 2005) and was amended to include the name “Islamic Jihad Union” on April 29, 2008, published in the 73 F. Reg 30443-01 (May 27, 2008).

As stated at the June 17, 2015 status conference, I will address Mr. Muhtorov's request for specific, additional discovery and declassification in a separate order, after conducting one or more prefatory CIPA § 4 hearings on the subject. Accordingly, this matter will be set for a discovery conference, to be attended by the government and the defense, at which time the government should be prepared to address the CIPA § 4 hearing and process for moving toward the declassification of any *Brady* and related information material to the defense in this case. The conference will be conducted before a court reporter and under conditions that will allow it to be conducted as a closed hearing, should the need arise.

Dated November 19, 2015

s/John L. Kane
SENIOR U.S. DISTRICT JUDGE

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 3

Vol. 11: 264-267

(Issue I)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Action No. 12-cr-0033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JAMSHID MUHTOROV and
BAKHTIYOR JUMAEV,

Defendants.

REPORTER'S TRANSCRIPT
(Status Conference)

Proceedings before the HONORABLE JOHN L. KANE, Judge,
United States District Court for the District of Colorado,
commencing at 3:15 p.m., on the 17th day of June, 2015, in
Courtroom A-802, United States Courthouse, Denver,
Colorado.

MARY J. GEORGE, FCRR, CRR, RMR
901 19th Street, Denver, Colorado 80294
Proceedings Reported by Mechanical Stenography
Transcription Produced via Computer

1 matters for case management resolution at the status
2 conference on June 17th, 2015, and I appreciate having
3 received it. I will tell you, however, that I only
4 received it about an hour and a half ago and I've already
5 prepared some matters for today's conference, so in the
6 future, if you do this, and I do appreciate it, but I'd
7 like to get it earlier so I can put it to better use.

8 I'm going to read my order into the record for
9 you. And, Ms. Fedasenka, if I go too fast, just tell me be
10 quiet.

11 THE INTERPRETER: I will. Thank you, Your
12 Honor.

13 THE COURT: Okay. All right. Among the various
14 pend- -- matters pending in this criminal action is
15 defendant's motion for notice of the surveillance
16 techniques utilized by the Government in its investigation
17 of the defendants. That's document 742. The motion is one
18 of several seeking information about the FISA, F-I-S-A,
19 authorized surveillance activity that led to the 2012
20 indictments of these defendants, Muhtorov and Jumaev, in
21 this case.

22 At first this activity was represented as being
23 limited to investigations conducted under FISA Title I and
24 FISA Title III, which I have already approved. In October
25 2013, the Government revealed that some of the information

1 it intends to use against Mr. Muhtorov was "incidentally
2 acquired" during surveillance [REDACTED]
3 [REDACTED] that was conducted under FISA Title VII.

4 Section 702 of Title VII, which was added by the
5 FISA Amendments Act of 2008, permits the warrantless
6 electronic surveillance of persons overseas "to acquire
7 foreign intelligence information" as long as the person is
8 reasonably believed to be located outside the United States
9 and as long as certain targeting and minimization protocols
10 to protect privacy and related interests of Americans here
11 and abroad are observed.

12 Section 702 authorizations received the imprimatur
13 of the FISA Court based on minimal representations by the
14 Executive, and judicial review of those authorizations is
15 limited to constitutional challenges such as the one before
16 me in the pending motion to suppress.

17 I am at present diligently working on an opinion
18 on defendants' motions to suppress this FAA-acquired data.
19 That's documents 520 and 521.

20 I take this status conference as an opportunity to
21 tell you what I'm going to do and what it means. My intent
22 at this point is to deny the motions to suppress, but to
23 put the Executive on alert in terms of justifying any
24 continued withholding on classified information grounds of
25 specific information related to the "incidental

1 acquisitions" of Mr. Muhtorov's communications and, in
2 particular, to receive a chronology from the Government of
3 how this activity took place and the time spent on each
4 such activity.

5 My holding with regard to the motion to suppress
6 will read something similar to the following language,
7 which is in draft form. And I quote from my own language
8 in draft form:

9 While I am convinced the FAA can be
10 unconstitutionally applied in domestic criminal
11 investigations, and most certainly is unconstitutionally
12 applied when used to capture and bank the international
13 communications of U.S. persons based solely on their
14 foreign contacts as in *Clapper*, I am equally convinced that
15 it was not unconstitutionally applied here. Based on my *in*
16 camera review of the classified and unclassified documents
17 made available to me, the FAA surveillance at issue was
18 narrowly tailored to the Government's foreign
19 intelligence-gathering prerogatives, and once Mr. Muhtorov
20 was identified as a U.S. person on U.S. soil, [REDACTED]
21 [REDACTED] authority to target him directly was
22 specifically and timely sought.

23 Mr. Jumaev has not been identified as an aggrieved
24 person for purposes of moving to suppress, and any facial
25 challenge he would have to the FAA would rise and fall with

1 that of Mr. Muhtorov's, even if he were found to have
2 standing.

3 That's the end of the draft quote.

4 The nature and scope of the CIPA, C-I-P-A, Section
5 4 hearing necessary to address pending discovery requests
6 is something I can discuss with the Government once the
7 opinion issues. It is, however, something Mr. Holloway
8 should start talking about with some urgency with his
9 agency associates.

10 There are pending motions for both Mr. Muhtorov
11 and Mr. Jumaev. Most are discovery related, such as
12 various motions for notice of the surveillance techniques
13 and interceptions used in this case, and those are
14 documents 458, 652, 653, and 658, and motions for
15 disclosure of statements the Government intends to use
16 against the defendants, documents 701 and 743.

17 There are also two motions to restrict that are
18 pending, documents 665 and 712, and a joint motion,
19 document 754, filed by the defendants to "unrestrict" a
20 reply brief they filed in support of their motion for
21 notice of surveillance techniques "so that the defendants
22 may treat this document as a public record consistent with
23 our country's tradition of open court proceedings."

24 There is also a motion, document 584, for an order
25 "requiring the Government to disclose or provide counsel

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 4

Vol. 1: 479-483

(Issue II)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Case Number 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. JAMSHID MUHTOROV, and
2. BAKHTIYOR JUMAEV,

Defendants.

ORDER ON PENDING MOTIONS
REGARDING FISA-ACQUIRED EVIDENCE

Kane, J.

This matter is before me on the following Motions:

- Defendant Muhtorov’s Motion to Suppress FISA Acquired Evidence for Purposes of Detention (Doc. 14) and related Supplement (Doc. 125); and
- Defendant Jumaev’s Combined FISA-related Motions: (1) to Adopt Defendant Muhtorov’s Supplemented Motion to Suppress; (2) for Disclosure Of FISA Materials; (3) for a Preliminary Challenge To Suppress FISA Acquired Evidence; and (4) for Leave To File A *Franks* Motion After Receipt All The Government’s Discovery (Doc. 157).

Defendants seek disclosure of all applications, orders, and related materials obtained pursuant to the Foreign Intelligence Surveillance Act, as amended (“FISA”); suppression

of information obtained or derived pursuant to FISA; and leave to file a motion for an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). In consequence and pursuant to statute, the government has filed an affidavit in which the Attorney General of the United States swears that disclosure of the FISA-acquired evidence or an adversary hearing would harm the national security of the United States.

As the statutes require, I have conducted an *ex parte* and *in camera* examination of the Motions, the government's unredacted and sealed brief in support of nondisclosure, along with the affidavits and documents filed under seal and relevant to the Defendants' Motions. From this examination and review of applicable authorities cited by the government and the Defendants, as well as authorities produced by my own research, I conclude on that basis the electronic surveillance and physical searches at issue were lawfully authorized and conducted, that the FISA materials need not and should not be disclosed in the interests of national security, and that the fruits of the electronic surveillance and physical searches should not be suppressed at trial. Therefore, the several motions are DENIED.

First, I make note of a general reluctance on my part as a judge to engage in any *ex parte* judicial activity and do so only when required by law. While the responsibility of defense counsel to protect the rights of defendants cannot be overstated, it is important to note that in the context of defendants' rights to discover FISA-acquired evidence, it is not an exclusive responsibility. The court itself is charged to protect the rights of defendants and to assure fairness in all proceedings under attendant circumstances. The ambit or

extent of counsel's responsibility is not coterminous with that of the court and where Congress has determined in the best interests of national security to limit counsel's scope of inquiry, the court's vigilance in protecting defendants rights and insuring fairness rises to a level of scrutiny. I have undertaken this *ex parte* review required by 50 U.S.C. § 1806 (f) under that standard. It is the same standard used by the Foreign Intelligence Surveillance Court ("FISC"), meaning that I may not second-guess the Executive Branch's certification that the surveillance has a foreign intelligence objective. *In re Grand Jury Proceedings of the Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003). My charge is to conduct a *de novo* review of the FISA materials to determine if the surveillance authorization was based on appropriate probable cause. If disclosure of the FISA materials is not necessary to make an accurate determination of the legality of the collection and if I find the surveillance was lawfully authorized and conducted, the motion must be denied. 50 U.S.C. § 1806(g).

Having concluded my review under 50 U.S.C. § 1806(f), I do not find it necessary to disclose any of the documents or orders incident to the FISA applications. There is no indication of any irregularities, misrepresentations of fact, vague identifications of the persons involved or any significant amount of non-foreign intelligence data that would call into question adherence to the minimization standards contained in the FISA orders. The attested facts support a finding of probable cause to believe that Defendants Muhtorov and Jumaev, the targets of the requested surveillance, were agents of a foreign power as defined by statute. I find the application and attendant affidavits complete and

in proper form and that as to the one Defendant who is a United States person (for that matter as well the other Defendant who is not a United States person), the certifications are not clearly erroneous.

In sum, I find that all of the FISA orders and applications concerning these Defendants meet the standards set out in 50 U.S.C. § 1801 *et seq.* While I do not find it necessary in this case to resort to a finding of a “good faith” belief on the part of the government agents involved in obtaining the FISA warrants, there is no indication whatever of a lack of such good faith. Moreover, I find these same persons made a good faith effort at minimizing information concerning United States persons that was acquired through the surveillance efforts. Therefore, I conclude the FISA surveillance was lawfully authorized and legally conducted. There is no basis for permitting defense counsel to review the FISA materials and no need to order a *Franks* hearing.

Finally, I find no basis for deviating from the near unanimous view that FISA does not violate the Fourth Amendment. It is conceivable that an argument could be made that FISA cannot be used to circumvent the Fourth Amendment because the probable cause standard to obtain a search warrant for a criminal prosecution is more stringent than for a FISA order, but that situation does not exist here where the electronic surveillance is directed at the activities of a foreign power and its agents and the criminal prosecution is merely incidental to that dominant purpose.

For the reasons stated, Defendant Muhtorov’s Motion to Suppress (Doc. 14) and Supplement (Doc. 125), and the Combined FISA-Related Motions of Defendant Jumaev

(Doc. 157) are DENIED.

Dated September 24, 2012.

s/John L. Kane
SENIOR U.S. DISTRICT JUDGE

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 5

Vol. 3: 148-149

(Issue II)

Islamic Jihad Group.²⁵

As has already been disclosed, the FISA application at issue in this case was based in part on FAA surveillance and collection. Mr. Muhtorov contends the “incidental” acquisition of his communications and their subsequent retention, querying, and use in criminal proceedings brought against him, was unreasonable under the Fourth Amendment. I have already reviewed the FISA Court’s Title I and Title III approvals and concluded the searches and surveillance conducted under those approvals was lawfully authorized and conducted. I have since performed an exhaustive *in camera* and *ex parte* review of all relevant additional classified materials provided to me by the government, including supplemental classified materials prepared at my request. I conclude on the record before me that a proper and supported application was filed, and that the targeting and minimization procedures forwarded were tailored to the government’s legitimate foreign intelligence purposes and took into account the privacy interests of individuals whose communications would be incidentally acquired. Mr. Muhtorov’s Motion to Suppress Evidence Obtained or Derived under § 702 (Doc. 520) is DENIED. Because I find all legal criteria were met by the government to establish that the searches and surveillance at issue were lawfully authorized and conducted, there is no need to consider the “good faith” alternative basis for denying the Motion to Suppress.

²⁵ Notification of its designation appears at 70 Fed. Reg. 35332-01 (June 17, 2005) and was amended to include the name “Islamic Jihad Union” on April 29, 2008, published in the 73 F. Reg 30443-01 (May 27, 2008).

As stated at the June 17, 2015 status conference, I will address Mr. Muhtorov's request for specific, additional discovery and declassification in a separate order, after conducting one or more prefatory CIPA § 4 hearings on the subject. Accordingly, this matter will be set for a discovery conference, to be attended by the government and the defense, at which time the government should be prepared to address the CIPA § 4 hearing and process for moving toward the declassification of any *Brady* and related information material to the defense in this case. The conference will be conducted before a court reporter and under conditions that will allow it to be conducted as a closed hearing, should the need arise.

Dated November 19, 2015

s/John L. Kane
SENIOR U.S. DISTRICT JUDGE

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 6

Vol. 13: 716

(Issue III)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Action No. 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JAMSHID MUHTOROV and
BAKHTIYOR JUMAEV,

Defendants.

REPORTER'S TRANSCRIPT
MOTION TO DISMISS

Proceedings before the HONORABLE JOHN L. KANE, JR.,
Senior Judge, United States District Court for the District of
Colorado, commencing at 11:01 a.m., on the 31st day of January,
2017, in Courtroom A802, United States Courthouse, Denver,
Colorado.

THERESE LINDBLUM, Official Reporter
901 19th Street, Denver, Colorado 80294
Proceedings Reported by Mechanical Stenography
Transcription Produced via Computer

1 nature -- by the way, Dr. Khalid from Carleton College, I
2 bought his book, and I'm reading it now. And I don't know how
3 you get more expert than people doing that sort of thing,
4 writing the books and knowing about it, and I think it will
5 help the jury.

6 So the defendants' motions to suppress, as I said,
7 1151, 1152, 1154, and 1156, will be denied, as will the
8 Government's motion to exclude the testimony of Drs. Leo and
9 Obolsky, Document 1212, and the defendant's *Daubert* challenge
10 to Dr. Steinberg, Documents 1199 and 1206, and the Government's
11 expert-related discovery motion remain pending, and we need to
12 get that taken care of posthaste.

13 The defendants' joint motions relating to surveillance
14 techniques, reconsideration of the clarification of the FISA
15 and FAA rulings already make, Documents 1107, 1108, 1109, and
16 the Government's related motion *in limine*, Docket 1211, these
17 motions will be likewise denied. I will address the
18 Government's concerns regarding reference to surveillance
19 techniques and evidentiary objections generally as they occur
20 at trial.

21 Now, the laboring oar is with me on these motions to
22 dismiss Count 5 of the Third Superseding Indictment. And I'm
23 not going to even attempt to indicate what my ruling is on that
24 now, but I'll get to it just as quickly as I can, as well as
25 this omnibus ruling. I'll include, I think, the motion -- the

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 7

Vol. 12: 546-554

(Issue IV)

1 IN THE UNITED STATES DISTRICT COURT
2 FOR THE DISTRICT OF COLORADO

3 Criminal Action No. 12-cr-33-1-2-JLK

4 UNITED STATES OF AMERICA,

5 Plaintiff,

6 vs.

7 1. JAMSHID MUHTOROV and
8 2. BAKHTIYOR JUMAEV,

9 Defendants.

10 **REPORTER'S TRANSCRIPT**

11 Motion Hearing

12
13 Proceedings before the HONORABLE JOHN L. KANE, JR.,
14 Judge, United States District Court for the District of
15 Colorado, occurring at 10 a.m., on the 18th day of May, 2017,
16 in Courtroom A802, United States Courthouse, Denver, Colorado.

17 **APPEARANCES**

18 GREGORY HOLLOWAY, DAVID TONINI and BETH GIBSON,
19 Assistant U.S. Attorneys, 1225 17th Street, Suite 700, Denver,
20 Colorado, 80202, appearing for the Plaintiff.

21 BRIAN LEEDY, KATE STIMSON, Stimson, Glover, Stancil,
22 Leedy, LLC, 1875 Lawrence Street, Suite 420, Denver, CO, 80202,
23 720-644-8066 and WARREN WILLIAMSON, Office of the Federal
24 Public Defender, 633 Seventeenth Street, #1000, Denver, CO,
25 80202, 303-294-7002 for Defendant, Mr. Muhtorov.

1 THE COURT: Right. We're going to have another
2 argument after this, but I -- let's take a recess for
3 approximately 15 minutes, and then I will come back with my
4 ruling on this case, and then we will recess and come back at 1
5 o'clock, so that people can have something to eat, for the
6 other motion.

7 THE COURTROOM DEPUTY: All rise.

8 (Recess at 11:14 a.m.)

9 (In open court at 11:40 a.m.)

10 THE COURT: Thank you, and please be seated. Well, we
11 are all in agreement that this issue is governed by the Supreme
12 Court's opinion in *Barker vs. Wingo*, that's the extent of our
13 agreement.

14 The four factors which have been discussed by counsel,
15 and are contained in the motions, that have to be considered,
16 are the length of delay, the assertion of the right, the
17 reasons for the delay and the issue of prejudice.

18 I want to point out, however, that there are no
19 bright-line decisions, nor could there be, in considering any
20 case on the constitutional issue of denial of speedy trial as
21 there can be with the Speedy Trial Act and the statute, but
22 these rights are -- and the factors involved are correlative,
23 and that means that they have to be evaluated and then
24 considered in conjunction with one another.

25 So, for example, the length of the delay in this case

1 is something I have commented about previously, and it -- it --
2 it bothers me emotionally, and quite frankly, physically,
3 that -- to think of people being held in custody for the length
4 of time that Mr. Muhtorov and Mr. Jumaev have been held,
5 without having a trial on the merits of the charges against
6 him, and that -- that is, according to the language of
7 Mr. Justice White, in the *Barker* opinion, the mere fact of
8 being kept from one's loved ones is -- and being held in -- in
9 custody is -- is prejudicial, that's something that weighs very
10 strongly on the side of the defendant in this motion. It is
11 not the kind of prejudice that we think of in most instances,
12 of legal analysis of it precluding the assertion of a right,
13 but it's, and perhaps more importantly, more of a recognition
14 by the law, that there are other factors besides the law itself
15 that enure to the rights and the benefits of any human being,
16 and the cost in this case of this -- of this charge is high
17 indeed, in terms of the personal investment.

18 There's another factor that is not equal to that, by
19 any means, and I don't suggest that it is, by the fact that it
20 follows what I have just said, but I think we all have to
21 recognize that this particular case is one in which the
22 government, the defense and the Courts all struggle, but it's
23 in term of our jurisprudence is very near.

24 We didn't spend the years and the cases and the study
25 over decades on this kind of criminal charge. The term

1 terrorism was hardly ever used in our case law until the last
2 20 years or so. The other thing that we have to recognize is
3 the very nature of this case, and distinguish it from some
4 others, where there have been terrorism trials that have gone
5 rather quickly to court, to trial, or to some other
6 disposition, but this is not the *Moussaoui* case, as an example,
7 nor is it a case where someone is discovered on an airplane
8 with an explosive in his tennis shoe; a fairly cut-and-dry sort
9 of thing. This is a case that involves conspiracy, and it
10 involves an enormous amount of electronic generated data. So
11 it takes time. And going back to *Barker vs. Wingo*, I think
12 that certainly the length of delay, without further
13 explanation, by time alone, does weigh heavily in favor of the
14 movant, but when one applies reason, in the correlative basis
15 of that ground, I think it becomes more understandable as to
16 why the delay.

17 I agree with Mr. Williamson about the assertion of the
18 right to a speedy trial. It's one which has been with us and
19 present for a long time. In fact, on reflection, it's rather
20 interesting that if the Congress of the United States passes a
21 statute called the Speedy Trial Act, the recognition of speedy
22 trial is implicit in everything that we do, and therefore one,
23 I think, has the right to assert a denial of speedy trial, and
24 mere proceeding through numerous steps pretrial does not and
25 should not constitute any indication of a waiver of that right.

1 So in terms of assertion, I think that too, weighs in favor of
2 Mr. Muhtorov. I mentioned, partly, the prejudice that is
3 there.

4 Now, on the other hand, when I look at the reasons, in
5 the first instance, this case was filed and it has been
6 explained throughout these proceedings that the arrest of
7 Mr. Muhtorov was made, in a sense, under exigent circumstances;
8 in that, he was within feet of leaving this country, and the
9 need for the arrest was imminent. There has been some, in
10 previous hearings, references to the action of the government
11 in surveillance and looking at Mr. Muhtorov, perhaps from as
12 early as 2009, and I'm referring to some of the testimony of
13 Agent Hale, or one of his affidavits, his affidavit, in May of
14 2009, there's a, I think, physical surveillance and then in
15 January of 2010 there was further government investigative
16 surveillance, and it was -- I don't mean to belittle this, but
17 it wasn't until January of 2012 when the arrest took place.

18 So there's a three-year period of time when there was
19 investigation and surveillance taking place. But from 2012
20 until today, in 2017, the legal actions have -- have taken
21 place. Mr. Muhtorov was arrested in January of 2012, and then,
22 quite honestly, from the transcript of the testimony on the
23 Motion To Suppress, it's apparent that Mr. Jumaev was aware of
24 Mr. Muhtorov's arrest, and his arrest took place in March of
25 2015 --

1 MR. WILLIAMSON: Twelve.

2 THE COURT: Two thousand fifteen. Yes, 2015 -- excuse
3 me -- 2013. The ensuing period of time is what is of greatest
4 concern, and how do I correlate the reasons that this case has
5 taken so long? I'm not sure the first one is even legally
6 recognizable, but as I alluded to earlier, the charts on the
7 waters of terrorism cases are slim and few for the prosecution,
8 for the defense, I can assure you for the Court. There's one
9 volume I have referred to, produced by the Federal Judicial
10 Center, that relates experiences of other trial Judges that
11 gives me some indication of what a Judge is supposed to do in
12 these cases, but I will be totally candid and tell you that I
13 have had cases that -- trials that have lasted for as long as
14 five months, that were not as complicated as this case, and
15 they were based on established rules of law, and there was no
16 conflict between -- well, there was some in one of them,
17 national security interests and the interests of the
18 administrative of justice. But as Mr. Holloway pointed out,
19 this, among other things, it is what lawyers and Judges refer
20 to as a case of first impression, and that means truly that the
21 pathway is unchartered.

22 I have to consider what the government has done, and
23 how long it has taken the government, and what I want to say,
24 and probably comes down to this, bottom line, in terms of my
25 ruling on this motion; and that is, I don't see this as a

1 question of fault or of deliberate intent to delay, in which
2 case, while it would not, under any circumstance, be considered
3 as a sanction to grant a motion under the Sixth Amendment, it
4 is, nevertheless, one in which I find the government and its
5 counsel have been dedicated, and clearly this record shows,
6 beyond any dispute, the due diligence, the extraordinary
7 efforts of the defense counsel in this case.

8 So I don't see this as being delays that are caused by
9 the 25-dollar word is the logomachy of lawyers, but this isn't
10 a case, to put it in more understandable language of lawyers
11 looking at an hourglass and wanting to examine each and every
12 grain of sand. It's one in which the necessities of the case
13 have required motions. The necessities of the case require
14 intense discovery, and that is further complicated by the fact
15 that there are some language difficulties, and the translation
16 of documents and a multitude of electronically generated data.
17 This -- this puts an antitrust case to shame, when it -- can
18 you get that?

19 *THE INTERPRETER:* I'm sorry. The last part.

20 *THE COURT:* Yeah. If you compare this with an
21 antitrust case, this one is very large in comparison.
22 Antitrust cases are civil cases, and some criminal, that they
23 are known and their reputation is to be very complicated, but
24 frankly, compared with this, they are elementary. So the
25 difficulty of the case itself is something that relates to the

1 delay.

2 I'm not entirely satisfied that the cases received the
3 kind of priority, in terms of providing discovery that it
4 needs. I once said, in one of the hearings, and it's been
5 brought back to me in the motions that I said that there was
6 delay and it was perhaps deliberate. I don't want to be
7 misinterpreted by that statement. What I meant was that I
8 think the government has a basket of priorities, and that they
9 thought out what they had to do, and make the decisions as to
10 gathering the information, and then how to comply with the
11 Classified Information Protection Act, and anticipating whether
12 this case was actually going to go to trial or not. What I can
13 only surmise was a factor that meant that the translations were
14 not done as soon as they could have been, but I don't know that
15 for a fact.

16 What I do know, for a fact, is that the reasons for
17 the length of time this is taking are palpable and legitimate
18 reasons. Now, it's been mentioned that I may have said this
19 same thing myself in terms of the necessity of having
20 Mr. Muhtorov, if he wants to call Mr. Jumaev to the stand, wait
21 until after Mr. Jumaev's trial, a Hobson's choice, and I think
22 it's unfortunate that I said it, because it really isn't a
23 Hobson's choice. It's a very difficult choice to make, and I
24 certainly am not trying to belittle the importance of
25 Mr. Muhtorov having to decide whether to remain in custody for

1 another six or seven months because of that decision. But the
2 fact is, is that Mr. Jumaev is entitled to a fair trial, and he
3 is entitled to exercise his right under the Fifth Amendment,
4 and when you relate these two matters and try to give fairness
5 to both defendants, the only rational way is to say, If you
6 want to call him to the stand, and you certainly may, you have
7 to wait until his trial. And his attorneys have a very
8 legitimate reason for saying that it takes them a long time to
9 go through the plethora, the glut, of information that they
10 have to in order to represent their client.

11 Now, there's one further thing I want to say about --
12 about this, and that is, I granted the severance, and I did so
13 with a full understanding of the importance to the defense of
14 Mr. Muhtorov's defense of Mr. Jumaev's testimony. It is not
15 something that I look at as being raised as a technicality.
16 It's -- Mr. Williamson pointed out, quite clearly, it's a jury
17 question, and that's true. Whether the jury will accept
18 Mr. Jumaev's testimony or not is a matter for the jury, not for
19 the Court, but it certainly is important, and it weighs heavily
20 in terms of a decision that has to be made about whether to go
21 to trial or not, before or after Mr. Jumaev's trial. I only
22 say that we're ready to go to trial, and as I have already
23 said, if Mr. Muhtorov wants a continuance, in order to have
24 Mr. Jumaev's testimony, I have already indicated that I would
25 grant that, but I think, in sum, that the reasons for the delay

1 in this case, as regrettable as they are, are justifiable, and
2 so the motion is denied.

3 Now, I think it's not out of place to tell you that
4 I'm well aware of what delay does, and I am not happy about
5 that. Our literature is replete with criticisms of our legal
6 system that -- think of Dickens' Bleak House, the case of
7 Jarndyce vs. Jarndyce, which lasted for so long, nobody knew
8 how or why it started, that's a pretty good point, criticism.

9 I'm also aware that someone of even greater talent,
10 Shakespeare, listed, *The law's delay is the second reason that*
11 *justified suicide*, and the only thing he said was that *since we*
12 *don't know what will happen on the other side, that makes --*
13 *conscience makes cowards of us all*. But he was looking at the
14 law's delay as one of the reasons; that's been with us. It's
15 been with us from the beginnings of trials.

16 What I will say in justification or in defense, if I
17 can, of our legal system, is that this is, at least, a nation
18 that spends this kind of energy in the search for justice;
19 whether it's obtainable or not is another matter. But the
20 intent is there, and I think the actions that have been taken
21 so far are reasonable. It is with that, that I deny the Motion
22 To Dismiss, and we will come back at -- it's snowing outside,
23 in case anyone outside the State of Colorado would be surprised
24 that it's late May and snowing, but nevertheless, it is. So we
25 will recess until 1:30, rather than 1 o'clock.

UNITED STATES v. MUHTOROV

Tenth Circuit Court of Appeals

Case No. 18-1366

ATTACHMENT 8

Vol. 20: 147-150

(Issue IV)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Action No. 12-cr-00033-JLK-1

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JAMSHID MUHTOROV,

Defendant.

REPORTER'S TRANSCRIPT
TRIAL TO JURY
DAY ONE

Proceedings before the HONORABLE JOHN L. KANE, JR.,
Senior Judge, United States District Court for the District of
Colorado, commencing at 9:03 a.m., on the 24th day of May,
2018, in Courtroom A802, United States Courthouse, Denver,
Colorado.

THERESE LINDBLUM, Official Reporter
901 19th Street, Denver, Colorado 80294
Proceedings Reported by Mechanical Stenography
Transcription Produced via Computer

1

A P P E A R A N C E S

2

3

4

GREGORY HOLLOWAY and JULIA MARTINEZ, Assistant U.S. Attorneys, 1801 California Street, Suite 1600, Denver, Colorado 80202, appearing for the Government.

5

6

7

WARREN WILLIAMSON, Assistant Federal Public Defender, 633 17th Street, 10th Floor, Denver, Colorado 80202, appearing for Defendant Muhtorov.

8

9

10

BRIAN LEEDY and KATHRYN STIMSON, Attorneys at Law, Haddon Morgan & Foreman, P.C., 150 East 10th Avenue, Denver, Colorado 80203, appearing for Defendant Muhtorov.

11

12

P R O C E E D I N G S

13

(In open court at 9:04 a.m.)

14

15

THE COURT: Thank you. Good morning, and please be seated.

16

17

Before the jury comes in, I want you to advise first -- please swear in the interpreters. Very sorry.

18

(Interpreters sworn.)

19

THE COURT: Thank you both. I do appreciate this.

20

21

22

The jury has not yet been informed that they're jurors in this case. I'm going to tell them that. But there is a couple of other matters.

23

24

25

And I don't want to spend a lot of time on this now, but there was a motion to dismiss that was just filed yesterday. And I appreciate why it was filed, and I'm

1 certainly sorry that the witness is dead, but the motion is
2 denied.

3 And there is a -- an order that I had entered on
4 June 5, 2017, denying the previous motion. And in that
5 hearing, I had said that where there is extreme delay,
6 prejudice is presumed; but it's a rebuttable presumption. And
7 we talked about this in that bench ruling, but I want to point
8 out that what I held there applies here just as well. And that
9 is that this case has been six years in preparation, it
10 involves the review and study of voluminous evidence, and it
11 has been further complicated by the need for translations
12 and -- accurate translations and contests involving
13 translations. And the pretrial litigation, as I've indicated
14 in the past, I've already signed in these -- this case and
15 Mr. Jumaev's case over 1,000 orders during this period of time.
16 And the case has always been one of great difficulty from the
17 beginning, because it involves on the one hand, national
18 security that has to be counterbalanced by the obligation to
19 present a fair trial.

20 And the protection of national security interests and
21 the interests of a fair and transparent trial are not always
22 compatible. And, indeed, that's one of the things that a judge
23 in a case of this nature has to do, is to draw lines which, in
24 the absence of considerable briefing and considerable research
25 on the Court's own part, would be arbitrary. But drawing the

1 line and also recognizing something that I think needs to be
2 emphasized is that this case involves matters of first
3 impression. And so there is no binding precedent from the
4 Supreme Court or the Court of Appeals on one of the critical
5 issues involving this conflict between national security and
6 transparency and due process and trials.

7 I have made that decision. And I'm sure it's going to
8 be reviewed -- if not in this case, in another -- by a higher
9 court. But I think that the complexities of the case, the
10 matters of first impression, the confrontation of national
11 security with the administration of justice are all matters
12 that militate and justify under the *Wingo* case the time that
13 has been spent.

14 I never found, nor do I find now, any evidence of --
15 at all of the prosecution attempting to delay this matter in
16 order to obtain some sort of advantage. It is unfortunate that
17 this witness died, but the witness does -- there is a proffer
18 that's made by the defense as to her testimony. And looking at
19 that proffer, it does not go to the gravamen of the charge. It
20 goes to an explanation of motivation and of background and not
21 to the essence of the charge.

22 So I think that may or may not be something that can
23 be worked out by the -- by making an offer of proof, as
24 distinguished from a proffer, and see what the government's
25 position is about admitting that statement from the

1 now-deceased witness.

2 I want to point out one further thing that I did at
3 that hearing and reading over the transcript of it earlier this
4 morning. And I -- I don't mean to suggest for a nanosecond
5 that this is some sort of self-laudatory thing, it's a matter
6 of the attorneys and the support groups that the attorneys
7 have, but it's also a matter of a fundamental description of
8 our system, and that is that the effort that has gone into the
9 preparation and the actual trial in these cases to my reckoning
10 exceeds that done in any other country. The time that has been
11 spent, the importance that it's given, and the dignity and
12 integrity of the judicial/legal process is something that
13 certainly everyone here in the well of the court knows has been
14 done in this case.

15 So the fact that we are thorough, the fact that we are
16 mincing in our analyses, is such that I think that we should
17 proceed to trial. And the record has been made by the defense
18 moving to dismiss for denial of speedy trial. But I think
19 under the *Barker v. Wingo* case that governs this -- and,
20 frankly, this is a matter of analysis even without that
21 guidance -- that the efforts that have been gone into this
22 case, the complexity of it, the voluminous nature of it, and
23 the novelty of issues of law are such that the delays have been
24 necessary.

25 Now, the next thing is, I debated having counsel to