[Oral Argument Requested]

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
District Court No. 1:12-cr-00033-JLK-1

BRIEF FOR THE UNITED STATES

JASON R. DUNN
United States Attorney

JAMES C. MURPHY
Assistant U.S. Attorney
District of Colorado

JOHN C. DEMERS
Assistant Attorney General

JOSEPH PALMER
STEVEN L. LANE
Attorneys
National Security Division
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
202-353-9402
Joseph.Palmer@usdoj.gov

RULE 26.1(B) DISCLOSURE STATEMENT

The government is not aware of any organizational victims to the criminal activity charged in this case.

TABLE OF CONTENTS

Page

RULE 26.1(B) DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES vi

GLOSSARY xii

PRIOR OR RELATED APPEALS 1

STATEMENT OF THE ISSUES 1

STATEMENT OF THE CASE 2

A. Introduction 2

B. The Islamic Jihad Union 2

C. Muhtorov Supports the IJU and Swears Allegiance To It 3

D. Muhtorov Prepares to Travel Abroad To Join the IJU 6

E. Final Planning and Arrest 8

F. Charges 8

G. Notice of Traditional FISA and Section 702 Surveillance 9

H. FISA Litigation in District Court 11

I. Conviction and Sentence 12

SUMMARY OF ARGUMENT 12

ARGUMENT 14

I. The Section 702 Surveillance in this Case Was Lawful under the Fourth Amendment 14

A. Introduction and Standard of Review 14

B. The Legal Framework for Foreign Intelligence Collection 15

1. The FISA Amendments Act.....15

2. Implementing Section 702 18

C. No Judicial Warrant Is Required for Section 702 Collection Under Well-Recognized Exceptions to the Warrant Requirement 20

1. A Warrant Is Not Required To Conduct Foreign-Intelligence Surveillance Targeting Non-U.S. Persons Located Abroad 22

2. Incidental Collection Does Not Trigger a Warrant Requirement 24

3. The Foreign Intelligence Exception Applies 26

D. The Section 702 Collection In this Case was Lawful Under the Fourth Amendment's Reasonableness Test 28

1. Section 702 Collection Advances the Government's Compelling Interest in Obtaining Foreign Intelligence Information to Protect National Security 29

2. The Privacy Interests of U.S. Persons Are Protected by Stringent Safeguards and Procedures 31

3. Section 702 Collection Has Sufficient Particularity.....35

4. The Special Minimization Rules Under FISA § 1802 Do Not Apply.....36

5. The Fourth Amendment Permits Queries Using Search Terms Associated with U.S. Persons Pursuant to Court-Approved Procedures 38

E. The FISC's Role in Reviewing Section 702 Procedures is Consistent with Article III 46

F. The Good Faith Exception to the Exclusionary Rule Applies 49

II. The District Court Properly Withheld the FISA Materials from Defense Counsel 49

III. Muhtorov Is Not Entitled to Disclosures About Other Techniques that He Speculates the Government Might Have Used In its Investigation 51

A. Standards of Review 53

B. The Government's Discovery and Disclosure Obligations Do Not Extend to the Additional Information Demanded by Muhtorov 53

1. The Disclosures Demanded by Muhtorov Are Not Required by the Constitution 54

2. Fed. R. Crim. P. 16 Does Not Support Muhtorov's Demand ...58

3. Muhtorov Is Not Entitled to Relief Under 18 U.S.C. § 3504 ...60

C. The District Court Did Not Abuse its Discretion in Conducting Ex Parte Proceedings Under FISA and CIPA 64

IV. The Delay In Bringing Muhtorov To Trial Was The Result Of the Complexity of the Case And His Own Litigation Strategy 70

A. The Issue Below and Standard of Review 71

B. Argument 71

1. Length of the Delay 71

2. Reasons for the Delay 72

3. Whether Muhtorov Asserted His Right to a Speedy Trial 76

4. Prejudice.....76

CONCLUSION.....81

ORAL ARGUMENT STATEMENT.....81

CERTIFICATE OF COMPLIANCE.....82

CERTIFICATE OF DIGITAL SUBMISSION.....83

CERTIFICATE OF SERVICE.....84

TABLE OF AUTHORITIES

Cases **Page**

Alderman v. United States, 394 U.S. 165 (1969)..... 54-55

American Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015).....57

In re Application of the FBI for an Order Requiring the Production of Tangible Things, 2013 WL 5741573 (FISC Aug. 29, 2013).....52

Barker v. Wingo, 407 U.S. 514 (1972) 71-72

Berger v. New York, 388 U.S. 41 (1967) 55

Block v. Rutherford, 468 U.S. 576 (1984) 78

Boroian v. Mueller, 616 F.3d 60 (1st Cir. 2010) 41

Brady v. Maryland, 373 U.S. 83 (1963) 53

Bruton v. United States, 391 U.S. 123 (1968) 75

[Caption Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011) 27, 32, 35, 48

Carpenter v. United States, 138 S. Ct. 2206 (2018).....56

City of Los Angeles v. Patel, 135 S. Ct. 2443 (2015) 47-48

Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).....10, 16, 20, 27, 32

Dalia v United States, 441 U.S. 238 (1979) 55

Davis v. United States, 564 U.S. 229 (2011) 49, 57

Degen v. United States, 517 U.S. 820 (1996).....53

In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008) 25-27, 29, 34, 36

Doggett v. United States, 505 U.S. 647 (1992)..... 71-72

Illinois v. Krull, 480 U.S. 340 (1987) 49

Illinois v. McArthur, 531 U.S. 326 (2001).....28

Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982).....41

Jencks v. United States, 353 U.S. 657 (1957).....55

Johnson v. Quander, 440 F.3d 489 (D.C. Cir. 2006) 41

Kentucky v. King, 563 U.S. 452 (2011) 22

Kolod v. United States, 390 U.S. 136 (1968).....55

Maryland v. King, 569 U.S. 435 (2013) 28, 36, 41

Mistretta v. United States, 488 U.S. 361 (1989)..... 46-47

Murray v. United States, 487 U.S. 533 (1988) 45

Nat'l Treas. Employees Union v. Von Raab, 489 U.S. 656 (1989) 20-21

Pennsylvania v. Mimms, 434 U.S. 106 (1977).....21

Pennsylvania v. Ritchie, 480 U.S. 39 (1987).....53

[Redacted], 402 F. Supp. 3d. 45 (FISC 2018).....40, 42

Riley v. California, 573 U.S. 373 (2014).....42

Roviaro v. United States, 353 U.S. 53 (1957).....66

In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) 46

Smith v. Maryland, 442 U.S. 735 (1979).....57

Terry v. Ohio, 392 U.S. 1 (1968).....21

United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010) 65

United States v. Alderisio, 424 F.2d 20 (10th Cir. 1970) 55

United States v. Alvillar, 575 F.2d 1316 (10th Cir. 1978).....63

United States v. Amawi, 695 F.3d 457 (6th Cir. 2012).....66, 68

United States v. Apperson, 441 F.3d 1162 (10th Cir. 2006).....65

United States v. Apple, 915 F.2d 899 (4th Cir. 1990).....62

United States v. Asgari, 940 F.3d 188 (6th Cir. 2019) 67

United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982) 51

United States v. Bowers, 847 F.3d 1280 (10th Cir. 2017).....53

United States v. Cash, 733 F.3d 1264 (10th Cir. 2013).....15

United States v. Daoud, 755 F.3d 479 (7th Cir. 2014) 50-51

United States v. Duka, 671 F.3d 329 (3d Cir. 2011) 26

United States v. El-Mezain, 664 F.3d 467 (5th Cir. 2011) 50-51

United States v. Frias, 893 F.3d 1268 (10th Cir. 2018) 78

United States v. Hanna, 661 F.3d 271 (6th Cir. 2011) 66

United States v. Hasbajrami, 2017 WL 1029500 (E.D.N.Y. Mar. 8, 2016) 36

United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019).....passim

United States v. Hicks, 779 F.3d 1163 (10th Cir. 2015).....71-72, 76-78

United States v. Leon, 468 U.S. 897 (1984) 49, 58

United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004) 30

United States v. Lustig, 830 F.3d 1075 (9th Cir. 2016).....43

United States v. Lustyik, 833 F.3d 1263 (10th Cir. 2016) 53, 65

United States v. Maranzino, 860 F.2d 981 (10th Cir. 1988) 59

United States v. Medina, 918 F.3d 774 (10th Cir. 2019).....79

United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982) 47

United States v. Mejia, 448 F.3d 436 (D.C. Cir. 2006) 68

United States v. Mohammad, 339 F. Supp. 3d 724 (N.D. Ohio 2018) ..25, 30, 52, 60

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

United States v. Mohamud, 666 F. App'x 591 (9th Cir. 2016) 50

United States v. Mohamud, 2014 WL 2866749
(D. Or. June 24, 2014).....27, 46, 48, 50

United States v. Muhtorov, 702 F. App'x 694 (10th Cir. 2017)..... 72, 76-77

United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008).....30

United States v. Pringle, 751 F.2d 419 (1st Cir. 1984) 68, 70

United States v. Robins, 978 F.2d 881 (5th Cir. 1992).....61, 64

United States v. Santiago, 46 F.3d 885 (9th Cir. 1995).....59

United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988) 66-67

United States v. Sedaghaty, 728 F.3d 885 (9th Cir. 2013) 42-43, 65, 68

United States v. Shelton, 30 F.3d 702 (6th Cir. 1994).....63

United States v. Simpson, 845 F.3d 1039 (10th Cir. 2017) 59

United States v. Sorensen, 801 F.3d 1217 (10th Cir. 2015) 53

United States v. Soto-Zuniga, 837 F.3d 992 (9th Cir. 2016) 60

United States v. Spagnuolo, 549 F.2d 705 (9th Cir. 1977).....59

United States v. Thompson, 866 F.3d 1149 (10th Cir. 2017) 57

United States v. United States District Court (*Keith*), 407 U.S. 297 (1972).....27, 55

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) 22-23, 26

United States v. Winder, 557 F.3d 1129 (10th Cir. 2009) 15

Zadvydas v. Davis, 533 U.S. 678 (2001) 23

Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975).....26

Statutes

18 U.S.C. app. 3 § 4 65-69

18 U.S.C. app. 3 § 6 67

18 U.S.C. § 2339B 9, 12

18 U.S.C. § 2510..... 60-61

18 U.S.C. § 3504..... 60-63

50 U.S.C. §§ 1801 .....passim

50 U.S.C. § 1802..... 36-38

50 U.S.C. § 1803 9

50 U.S.C. § 1804 9

50 U.S.C. § 1805 9

50 U.S.C. § 1806 .....45, 49, 64, 74

50 U.S.C. § 1821 .....9, 48

50 U.S.C. § 1823 9

50 U.S.C. § 1824 9

50 U.S.C. § 1825 64

50 U.S.C. § 1861 52

50 U.S.C. § 1881a .....passim

50 U.S.C. § 1881e 45, 50, 64, 74

FISA Amendments Act of 2008, Pub. L. No. 110-261 .....15, 16

FISA Amendments Reauthorization Act, Pub. L. No. 115-118 .....10, 18, 39

Other Authorities

David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* (2019) 15

Executive Order No. 12,333 ..... 16, 54, 62-63

Fed. R. App. P. 28(i) 70

Fed. R. Crim. P. 16..... 58-60

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014).....19, 29, 33, 35, 39

GLOSSARY

CIPA.....Classified Information Procedures Act

DNI.....Director of National Intelligence

EO .....Executive Order

FBI.....Federal Bureau of Investigation

FISA .....Foreign Intelligence Surveillance Act

FISC .....Foreign Intelligence Surveillance Court

IJU .....Islamic Jihad Union

PAA.....Protect America Act

PCLOB.....Privacy and Civil Liberties Oversight Board

ROA .....Record on Appeal

PRIOR OR RELATED APPEALS

This Court has considered two prior appeals in this case: *United States v. Muhtorov*, No. 17-1220; and *Muhtorov v. Choate*, No. 17-1252. The Court has procedurally consolidated this appeal with the appeal of codefendant Bakhtiyor Jumaev, No. 18-1296.

STATEMENT OF THE ISSUES

1. Whether the government violated the Fourth Amendment by acquiring communications of a non-United States person reasonably believed to be located outside the United States under Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a, where that surveillance incidentally acquired communications to which Muhtorov was a party.
2. Whether the district court abused its discretion in finding that disclosure to the defense of classified materials was unnecessary for the court to determine that the Section 702 surveillance was lawful.
3. Whether the district court abused its discretion in rejecting Muhtorov's demand for additional disclosures concerning surveillance techniques that he speculates the government might have used to investigate him.
4. Whether Muhtorov was denied his Sixth Amendment right to a speedy trial.

STATEMENT OF THE CASE

A. Introduction

On January 21, 2012, federal agents arrested Muhtorov as he boarded a flight to Turkey with a one-way ticket. ROA Vol. 20 at 400-01. Muhtorov was on his way to join a terrorist organization called the Islamic Jihad Union (IJU). ROA Vol. 16 at 207. He was carrying over $2,800 in cash, two brand-new iphones, and a new ipad. ROA Vol. 20 at 651, 709-14. He also had his personal cellphone, which was full of terrorist propaganda glorifying attacks on U.S. forces. *Id.* at 714, 820, 835-57.

Muhtorov had been communicating directly with the IJU for years. ROA Vol. 16 at 211. He had sent them his oath of allegiance, swearing that he stood ready to risk his life in jihad. *Id.* at 212 n.2. He had offered to send the IJU money and to upload propaganda videos. *Id.* at 212. And he had agreed to travel abroad and join the IJU's propaganda unit to help create and distribute the same kind of terrorist videos he had on his phone. ROA Vol. 20 at 482, 541-42. He hoped to become a terrorist fighter and die fighting for the IJU. *Id.* at 541-42.

B. The Islamic Jihad Union

The IJU is a violent, jihadist terrorist group. ROA Vol. 16 at 209-10. Its members are mostly from Uzbekistan. *Id.* The IJU opposes the Uzbek government from its bases in Pakistan's tribal areas. *Id.* The IJU also engages in

"global" jihad, including fighting against U.S. forces in neighboring Afghanistan. *Id.*; ROA Vol. 20 at 308-14. The IJU is affiliated with al Qaeda and the Taliban. *Id.* at 321. The IJU's men, some of whom were Soviet Army veterans, are among the most lethally effective fighters against U.S. forces in Afghanistan. *Id.* at 314-15. The IJU has also conducted and attempted terrorist attacks on U.S. embassies and other targets outside of Afghanistan. *Id.* at 308-09. In 2005, the State Department designated the IJU as a foreign terrorist organization. *Id.* at 817.

The IJU had an official website called "soldiqlar.com." ROA Vol. 20 at 317, 400, 818.[1] The IJU used sodiqlar.com to spread propaganda, raise money, and recruit followers to come to Pakistan to join the ranks. *Id.* at 318.

C. Muhtorov Supports the IJU and Swears Allegiance To It

In 2007, Muhtorov and his family were granted admission to the United States as refugees. ROA Vol. 16 at 210. They settled in Denver. ROA Vol. 20 at 397. In 2009, Muhtorov went to Philadelphia to study for a license to drive trucks. ROA Vol. 16 at 211. A mutual friend arranged for Muhtorov to stay with Bakhtiyor Jumaev, who was also from Uzbekistan. *Id*.

After Muhtorov returned to Colorado, he and Jumaev stayed in touch. *Id.* The two men discussed their growing interest in the IJU's violent ideology. *Id*. Muhtorov and Jumaev shared propaganda videos that they found online. *Id.* The

[1] "Sodiqlar" means "the truthful ones." ROA Vol. 20 at 1021.

two men used code words when they talked about terrorism. *Id.* "Wedding" meant fighting or jihad; the "wedding house" was the IJU's headquarters in Pakistan's tribal areas; "Switzerland" meant Afghanistan, a "wedding gift" was a contribution to a terrorist organization, and a fighter who "got married" had been killed and achieved martyrdom. ROA Vol. 20 at 977-84. Muhtorov also used anonymizing software when he accessed terrorist websites. ROA Vol. 20 at 463-67, 481, 873.

From 2009 until his arrest in January 2012, Muhtorov communicated directly with the IJU by sending messages to the administrator for the IJU's website, sodiqlar.com. ROA Vol. 16 at 211. Muhtorov and the administrator became friends. *Id.* They referred to each other as "brother" and "friend," and Muhtorov called himself the administrator's "humble servant." ROA Vol. 20 at 486, 531. Muhtorov sent the administrator pictures of himself and his children. ROA Vol. 20 at 485, 497.

On March 5, 2011, Muhtorov told the administrator that Jumaev had promised to give money to the IJU. ROA Vol. 20 at 436-37. The administrator responded that the IJU had "dire financial needs." *Id.* Jumaev mailed Muhtorov a check for $300, explaining that the contribution should "not be the last one" he and Muhtorov provided to the IJU. ROA Vol. 20 at 1021. Muhtorov deposited the check and asked the administrator how to forward the money. ROA Vol. 16 at

212. While Muhtorov was waiting for instructions, his wife spent the money on living expenses. *Id.* Muhtorov continued to ask the administrator how to send the $300. ROA Vol. 20 at 482.

A few days after receiving Jumaev's check, Muhtorov sent an email to the sodiqlar.com administrator swearing allegiance to the IJU. ROA Vol. 20 at 481-82. Muhtorov asked the administrator to witness his oath and deliver it to the IJU's leader. *Id.* In his oath, Muhtorov declared that he was "ready for any task, even if it means the risk of death." *Id.* at 482. Muhtorov continued, "I am ready to perform [jihad] by offering possessions and committing pilgrimage if ordered. I am ready for any Sharia[2] order." *Id.* at 482-83, 986-87.

The IJU administrator responded that same day: "Brother, may God be pleased and bless your oath of allegiance." ROA Vol. 20 at 483. The administrator said he would "deliver the message to our leader." *Id.* As for Jumaev's $300, the administrator asked Muhtorov to "hold on a little" so the administrator could "find out from the brothers the way to handle it." *Id.*

A few weeks later, Muhtorov reminded the administrator that Jumaev had sent him $300, "entrusting it to me for a wedding gift." ROA Vol. 20 at 484. In later communications, Muhtorov continued asking for instructions about delivering money. ROA Vol. 20 at 486.

[2] "Sharia" means Islamic law. ROA Vol. 20 at 987.

Muhtorov also discussed helping the IJU with an FBI confidential informant who Muhtorov believed was a like-minded IJU supporter. ROA Vol. 20 at 736. Muhtorov told the informant that Jumaev had sent him $300 for the IJU, but the IJU had still not told him how to deliver it. ROA Vol. 16 at 212.

Through the administrator, the IJU tasked Muhtorov to upload and distribute terrorist propaganda and to help the IJU acquire satellite internet equipment. *Id.* at 212-13; ROA Vol. 20 at 509-10. Muhtorov told the informant that he was helping the IJU upload videos on the internet, and he asked the informant to help him distribute the IJU's propaganda. *Id.*

D. Muhtorov Prepares To Travel Abroad To Join the IJU

After Muhtorov swore allegiance to the IJU, he began preparing to leave the United States to join the organization. Muhtorov discussed his plan to go "to the wedding" with Jumaev, the IJU administrator, and the informant. ROA Vol. 16 at 213-14; ROA Vol. 20 at 484-87. Muhtorov talked about the "wedding gifts"—money and electronic devices—that he planned to bring. *Id.* at 526-27. At first, Muhtorov hoped to receive a personal order from the IJU's leader. *Id.* at 484. When the "wedding invitation" did not immediately arrive, Muhtorov told the administrator that he would come anyway. *Id.* at 486-87. The administrator responded that the IJU was "very happy" to learn that Muhtorov was coming. *Id.*

The administrator assured Muhtorov: "We will be waiting for you. Have a safe trip." *Id.*

Jumaev supported Muhtorov's plan. ROA Vol. 20 at 492 ("I envy you. You, too, are leaving to a wedding. I want to go to the wedding too."). Later, Jumaev said, "You're going to die either way," but "death over there is better." *Id.* at 522-23. Muhtorov replied, "It is so." *Id.*

Muhtorov planned to go to Turkey first and then continue "further on" to the "wedding house" at the IJU's headquarters in Pakistan's tribal areas. ROA Vol. 20 at 978-79. Muhtorov considered taking his family with him, but he decided to go alone and have his family follow later. ROA Vol. 20 at 487; ROA Vol. 16 at 214.

The IJU wanted Muhtorov to work in its propaganda and recruitment unit. ROA Vol. 16 at 214. But Muhtorov's ultimate goal was to become a martyr by dying in combat. He told his friend Mustafa that he wanted to fight with a "weapon in one hand and with the Quran in the other." ROA Vol. 20 at 1013. He declared that he would "accept martyrdom." ROA Vol. 20 at 542. In a call with his daughter, he asked her to pray for him to become a martyr: "Remember, I told you to pray for your Daddy to become a martyr . . . Don't pray, 'Don't let him leave!' It will be a curse for me . . . Pray and say, 'Make my father a martyr, one of [the] real martyrs." ROA Vol. 20 at 504-05.

E. Final Planning and Arrest

On January 16, 2012, Muhtorov bought a one-way ticket to Istanbul to depart on January 21. ROA Vol. 16 at 216. He shaved his beard to avoid suspicion at the airport. ROA Vol. 20 at 543-44. Muhtorov instructed his wife to prepare to leave by obtaining their tax refund, selling their furniture, and buying tickets for her and the children to travel to Turkey. *Id.* at 550-51.

On January 21, 2012, Muhtorov took a cab to O'Hare Airport in Chicago. ROA Vol. 16 at 214-15. On the way, he bought "wedding gifts" —a new iPad and two new iPhones. ROA Vol. 20 at 714, 820, 835-57. His personal cellphone was full of violent terrorist videos. ROA Vol. 16 at 215. He was carrying $2,865 in cash. ROA Vol. 20 at 714.

The FBI arrested Muhtorov after he passed through security. ROA Vol. 20 at 559-60. After waiving his *Miranda* rights, Muhtorov admitted that he had been communicating with the IJU's website administrator and that he knew the IJU was a terrorist organization. *Id.* at 561-65; ROA Vol. 16 at 215.

F. Charges

A grand jury charged Muhtorov with four counts of conspiring and attempting to provide material support to a designated foreign terrorist

organization, in violation of 18 U.S.C. § 2339B. ROA Vol. 1 at 269-72.[3] The alleged material support included money, personnel (including himself), and communications equipment and services. *Id.*

G. Notice of Traditional FISA and Section 702 Surveillance

Before trial, the government filed a notice advising Muhtorov that the government intended to offer into evidence "information obtained and derived from electronic surveillance and physical searches conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, 50 U.S.C. §§ 1801-1811 and 1821-1829." ROA Vol. 1 at 220. Those provisions, referred to here as "traditional" FISA authority, permit certain electronic surveillance and physical searches based on an order from the Foreign Intelligence Surveillance Court (FISC). Before the FISC may issue a traditional FISA order, the FISC must find, among other things, probable cause to believe that the target is a foreign power or its agent. *See* 50 U.S.C. §§ 1801, 1804-05, 1821, 1823-24.[4]

On October 25, 2013, the government filed a supplemental pretrial notice advising Muhtorov that some of the previously noticed FISA evidence was itself derived from information acquired pursuant to Section 702 of FISA, 50 U.S.C.

---

[3] Jumaev was charged in the same indictment.

[4] FISC judges are United States District Judges designated by the Chief Justice. 50 U.S.C. § 1803(a).

§ 1881a. ROA Vol. 1 at 552. As discussed below, Section 702 was enacted in 2008 to augment traditional FISA by establishing supplemental procedures for authorizing targeted surveillance for intelligence purposes of foreign persons located outside the United States with the assistance of U.S. electronic communication service providers. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 404-06, 422 (2013). Under Section 702, instead of issuing traditional FISA orders, the FISC approves annual certifications that specify categories of foreign intelligence information the government is authorized to acquire and the procedures governing the collection. 50 U.S.C. § 1881a(h), (j).[5] The FISC must find, among other things, that the "targeting procedures," which ensure that the authorized surveillance is properly aimed at non-U.S. persons located outside the United States, are consistent with the statutory standards and the Fourth Amendment. *Id.* § 1881a(j)(2)(B), (j)(3). The FISC also must find that the "minimization procedures," which restrict how the government treats information of U.S. persons who may communicate with the foreign targets, are likewise consistent with the statute and the Fourth Amendment. *Id.* § 1881a(j)(2)(C), (j)(3).

[5] Congress amended Section 702 in 2018. *See* FISA Amendments Reauthorization Act, Pub. L. No. 115-118, 132 Stat. 3 (Jan. 19, 2018) ("2018 Reauthorization Act"). The citations in this brief are to the current statute.

H. FISA Litigation in District Court

In this case, the government acquired under Section 702 the communications of a non-U.S. person abroad and, in so doing, incidentally collected communications to which Muhtorov was a party. *See* Appellant's Add. at 148. The government used some of these incidentally collected communications to support its application for traditional FISA orders. *Id.* The fruits of that traditional FISA collection were therefore partially "derived from" information collected under Section 702. Evidence obtained and/or derived from that traditional FISA collection was, in turn, used at trial.

Muhtorov moved to suppress the Section 702-derived evidence. After reviewing the relevant material in camera and ex parte, the district court found that the Section 702 collection here was constitutionally reasonable. Appellant's Add. 148. The court weighed the government's "legitimate" interest in "using intelligence information to detect and prevent criminal acts of terrorism," *id.* at 144, against the privacy interests of a "third party who is a participant in intercepted communications with a target overseas," *id.* at 141-42, and held that the statute's procedural safeguards, including FISC-approved targeting and minimization procedures, satisfied the Fourth Amendment, *id.* at 143-45. The court explained that Section 702 collection was "tailored to the very serious purpose of foreign intelligence gathering . . . and may not be used to target U.S.

persons," and that the minimization procedures sufficiently "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 statute and the Fourth Amendment. *Id.* at 145; *see also id.* at 148.

I. Conviction and Sentence

The jury convicted Muhtorov on three violations of 18 U.S.C. § 2339B, based on conspiring and attempting to provide material support to the IJU in the form of money and himself. The jury acquitted Muhtorov on one count based on providing communications equipment. The district court sentenced Muhtorov to 132 months of imprisonment. ROA Vol. 20 at 1673.

SUMMARY OF ARGUMENT

I. The district court properly denied Muhtorov's motion to suppress evidence derived from surveillance authorized under Section 702. The Section 702-authorized collection in this case, which targeted, for foreign intelligence purposes, a non-U.S. person located outside the United States with whom Muhtorov was communicating, was reasonable under the Fourth Amendment. First, the Fourth Amendment generally does not apply to non-U.S. persons abroad. The fact that surveillance targeting such persons also incidentally collects communications of U.S. persons does not trigger a warrant requirement under

well-established principles and precedent. Every court to review Section 702 surveillance has found the warrant requirement inapplicable. Alternatively, Section 702 surveillance falls within the "foreign intelligence exception" to the warrant requirement.

The Section 702 collection here also satisfied the Fourth Amendment's reasonableness standard. The government has an interest of the utmost importance in obtaining foreign intelligence information to protect the United States from foreign threats, including international terrorism. That interest outweighs the privacy interests of U.S. persons such as Muhtorov whose communications are incidentally collected, particularly where, as here, the government followed court-approved procedures reasonably designed to protect such privacy interests.

The Fourth Amendment permits the government to query, using search terms associated with U.S. persons, information it has lawfully collected under Section 702. Court-approved procedures reasonably restrict such queries to ensure they are done for proper purposes. Even if the government's actions in this case violated the Fourth Amendment, the good-faith exception to the exclusionary rule would apply.

II. The district court properly withheld classified FISA materials from the defense. FISA requires courts to review FISA materials in camera and ex parte unless disclosure is necessary to resolve the lawfulness of the collection. Courts

have uniformly upheld that process. The district court properly found that disclosure to the defense was not necessary here.

III. The district court did not abuse its discretion in denying Muhtorov's demand for additional disclosures concerning all surveillance techniques the government used to investigate him, including information about the timing and duration of each, the applicable legal authorities, and the evidence obtained. None of the authorities relied upon by Muhtorov supports his demand.

IV. The delay in bringing Muhtorov's case to trial did not violate his Sixth Amendment right to a speedy trial. The delay resulted principally from the complexity of the case—including voluminous discovery involving classified information and requiring translation—and from Muhtorov's aggressive litigation strategy. Muhtorov's speedy trial claim fails because (1) he was responsible for much of the delay; (2) he waited years before demanding a speedy trial; and (3) he cannot demonstrate significant prejudice.

ARGUMENT

I. The Section 702 Surveillance in this Case Was Lawful under the Fourth Amendment

A. Introduction and Standard of Review

Muhtorov contends that the district court erred in denying his motion to suppress evidence derived from Section 702 on the ground that collection of his communications under Section 702 violated the Fourth Amendment. Muhtorov

and amici challenge the government's authority to conduct critical foreign intelligence surveillance targeting non-U.S. persons outside the United States pursuant to court-approved procedures Congress has repeatedly authorized.

Section 702 surveillance lawfully targets non-U.S. persons abroad who lack Fourth Amendment rights. No warrant requirement applies—either to the foreign targets abroad or to third-party U.S. persons who communicate with them. And the surveillance here was constitutionally reasonable. Every court to reach the issue has held that surveillance under Section 702 is reasonable under the Fourth Amendment.

When reviewing a district court's denial of a motion to suppress evidence, this Court applies "a deferential sort of de novo review." *United States v. Winder*, 557 F.3d 1129, 1133 (10th Cir. 2009) (citation omitted). The Court considers the totality of the circumstances and views the evidence in the light most favorable to the government. *United States v. Cash*, 733 F.3d 1264, 1272 (10th Cir. 2013).

B. The Legal Framework for Foreign Intelligence Collection

1. The FISA Amendments Act

When FISA was enacted in 1978, it did not apply to most of the government's extraterritorial surveillance. *See* David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17:1 (2019). This was true even if that surveillance might specifically target U.S. persons abroad or

incidentally acquire, while targeting foreign nationals abroad, communications to or from U.S. persons or persons located in the United States. *See id.* Instead, surveillances or searches abroad were conducted under the President's inherent constitutional authority, pursuant to Executive Order 12,333.[6] *See id.* By 2008, however, as terrorists and other foreign intelligence targets abroad adopted new technologies that caused communications to transit this country, FISA's provisions required a traditional FISA court order in increasingly common circumstances for intelligence collection aimed at foreign persons abroad. *See id.*

In July 2008, Congress addressed this situation by enacting the FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436, which enacted a new Section 702 of FISA. Section 702 "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad." *Clapper*, 568 U.S. at 404-06.

Section 702 provides that, "upon the issuance" of an order from the FISC, the Attorney General and Director of National Intelligence ("DNI") may jointly authorize the "targeting of persons reasonably believed to be located outside the

[6] E.O. 12,333, as amended, addresses, *inter alia*, the government's "human and technical collection techniques . . . undertaken abroad." Exec. Order No. 12,333, § 2.2, 3 C.F.R. 210 (1981 Comp.), *reprinted as amended in* 50 U.S.C. § 401 note (Supp. II 2008).

United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). Section 702 specifies that the authorized acquisition may not intentionally "target a United States person"—whether that person is known to be in the United States or is reasonably believed to be outside the United States. 50 U.S.C. § 1881a(b)(1), (3). Under Section 702, the government also may not target a person outside the United States "if the purpose . . . is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2). Section 702 further requires that the acquisition be "conducted in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. § 1881a(b)(6).

Section 702 requires the government to obtain the FISC's approval of (1) a government certification regarding the proposed surveillance, and (2) targeting and minimization procedures to be used in the acquisition. 50 U.S.C. § 1881a(a), (c)(1), (i)(2)-(3); *see* 50 U.S.C. § 1881a(d)-(e). The Attorney General and DNI must certify that, among other things, (1) the acquisition does not violate the Fourth Amendment and complies with the statutory limitations that prohibit targeting United States persons or persons in the United States; (2) the acquisition involves obtaining "foreign intelligence information from or with the assistance of an electronic communication service provider"; (3) the targeting procedures are reasonably designed to ensure that any acquisition targets only persons reasonably believed to be outside the United States; and (4) the minimization procedures

appropriately restrict the acquisition, retention, and dissemination of nonpublic information about U.S. persons. 50 U.S.C. § 1881a(h)(2)(A)(i), (ii), (vi)-(vii).

The FISC must review the certification and the targeting and minimization procedures. 50 U.S.C. § 1881a(i)(1)-(2). If the FISC determines that the certification contains the required elements and that the procedures are "consistent with" the statutory requirements and "the [F]ourth [A]mendment," the FISC approves the certification and the use of the targeting and minimization procedures for a period of up to one year. 50 U.S.C. § 1881a(j)(3)(A); *see* 50 U.S.C. § 1881a(a).[7]

2. Implementing Section 702

The government acquires communications pursuant to Section 702 through compelled assistance from electronic communication service providers. 50 U.S.C. § 1881a(i). The government identifies to these service providers specific communications facilities, such as email addresses and telephone numbers, that the government has assessed, through the application of FISC-approved targeting procedures, are: (1) likely to be used by non-U.S. persons reasonably believed to be located abroad, (2) who possess, communicate, or are likely to receive a type of foreign intelligence information authorized for collection under a FISC-approved

[7] In 2018, Congress reauthorized Section 702 until December 31, 2023. *See* 2018 Reauthorization Act § 201(a), 132 Stat. 19.

certification. The government must identify specific communications facilities, not key words or the names of targeted individuals. See *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* ("PCLOB Report") 32–33; 41-46 (July 2, 2014).[8]

The FISC has approved a series of Section 702 certifications dating back to 2008. The FISC has found that acquisitions under Section 702 were not subject to the Fourth Amendment's warrant requirement because they target "persons reasonably believed to be located outside the United States," who are "not protected by the Fourth Amendment," and such targets "will have been assessed by [the government] to possess and/or to be likely to communicate foreign intelligence information." *In re DNI/AG Certification*, No. 702(i)-08-01 (FISC 2008) ("*FISC 2008 Op.*") Mem. Op. at 35, 37.[9] The FISC has also concluded that the acquisitions satisfied the Fourth Amendment's reasonableness requirement "in

[8] Available at https://www.pclob.gov/library/702-Report.pdf. The Privacy and Civil Liberties Oversight Board ("PCLOB") is an independent Executive Branch agency. The PCLOB found that the "core of the Section 702 program—acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight," was reasonable under the Fourth Amendment. PCLOB Report at 9.

[9] Available at http://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf.

view of the gravity of the government's national security interests and the other safeguards embodied in the targeting and minimization procedures." *Id.* at 38, 41.

Section 702 requires that the Attorney General and DNI periodically assess the government's compliance with targeting and minimization procedures and relevant compliance guidelines, and that they submit those assessments to the FISC and to Congressional oversight committees. *See* 50 U.S.C. § 1881a(m). In sum, "[s]urveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment." *Clapper*, 568 U.S. at 404.

C. No Judicial Warrant Is Required for Section 702 Collection Under Well-Recognized Exceptions to the Warrant Requirement

The acquisition of Muhtorov's communications, through traditional FISA orders that were predicated in part on Section 702 collection, did not violate the Fourth Amendment's warrant requirement. The Fourth Amendment prohibits "unreasonable searches" and provides that "no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Although the concepts of probable cause and a warrant requirement bear on the reasonableness of a search, "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." *Nat'l Treas. Employees Union v. Von Raab*, 489 U.S. 656, 665

(1989). The touchstone of Fourth Amendment analysis is "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security." *Pennsylvania v. Mimms*, 434 U.S. 106, 108-09 (1977) (per curiam) (quoting *Terry v. Ohio*, 392 U.S. 1, 19 (1968)).

Muhtorov argues (Br. 27) that the incidental acquisition of his communications pursuant to Section 702 collection targeting a non-U.S. person abroad "violated the Fourth Amendment's warrant requirement." But as the Ninth and Second Circuits unanimously held, the Fourth Amendment does not require a warrant where, as here, the government targets under Section 702 a non-U.S. person abroad even though such searches may incidentally collect some communications between the target and a U.S. person. *United States v. Mohamud*, 843 F.3d 420, 441 (9th Cir. 2016) (holding that "because the target of the surveillance was a non-U.S. person located outside of the United States at the time of the surveillance, the government was not required to obtain a search warrant to collect" the email communications of a U.S. person with the foreign national "as an incident to its lawful search of the foreign national's email" under Section 702); *United States v. Hasbajrami*, 945 F.3d 641, 664 (2d Cir. 2019) (same).[10] Muhtorov cites no contrary authority.

[10] As discussed below, the Second Circuit in *Hasbajrami* remanded for further factfinding related to any querying of databases containing Section 702 information that might have affected the case. The remand does not affect the

1. A Warrant Is Not Required To Conduct Foreign-Intelligence Surveillance Targeting Non-U.S. Persons Located Abroad

The Supreme Court has "inferred" from the Fourth Amendment that "a warrant must generally be secured" for government searches, but the Court has recognized reasonable "exceptions" from that "warrant requirement." *Kentucky v. King*, 563 U.S. 452, 459 (2011). In *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), the Supreme Court recognized one such exception for searches directed against aliens outside the United States. *Id.* at 266-67. The Court rejected a warrant requirement in that case because the Fourth Amendment does not "restrain the actions of the Federal Government against aliens outside of the United States" and thus does not "apply to activities of the United States directed against aliens in foreign territory." *Id.* at 266-67, 271; *see id.* at 263, 265. That limitation is consistent with decisions recognizing that "aliens receive [certain] constitutional protections when they have come within the territory of the United States and developed substantial connections with this country." *Id.* at 271; *see id.* at 275 (Kennedy, J., concurring) ("[T]he Constitution does not create, nor do general principles of law create, any juridical relation between our country and some undefined, limitless class of noncitizens who are beyond our territory."). *Verdugo-*

---

court's holding that the incidental collection did not require a warrant and was constitutionally reasonable.

Urquidez therefore reflects the "well-established" principle that Fourth Amendment protection is otherwise "unavailable" to "aliens outside of our geographic borders." *Zadvydas v. Davis*, 533 U.S. 678, 693 (2001). Disregarding that limitation "would have significant and deleterious consequences for the United States" in national security contexts. *Verdugo-Urquidez*, 494 U.S. at 273.

The Second and Ninth Circuits correctly applied those teachings in concluding that foreign nationals abroad whose communications the government targeted for Section 702 collection possessed no Fourth Amendment rights requiring a warrant. *See Hasbajrami*, 945 F.3d at 663; *Mohamud*, 843 F.3d at 439. And Muhtorov's argument (Br. 33) that a warrant should be necessary because the collection occurred within the United States is inconsistent with the Supreme Court's rationale in *Verdugo-Urquidez*. Muhtorov identifies no authority to justify requiring a warrant to conduct foreign-intelligence surveillance of an alien who is located abroad. As the Ninth Circuit explained, the critical Fourth Amendment factors are the overseas location and foreign nationality of the *target*, not "where the government literally obtained the electronic data." *Mohamud*, 843 F.3d at 439; *see also Hasbajrami*, 945 F.3d at 664-65.

If Muhtorov were correct, a warrant would be required to conduct any foreign-intelligence surveillance of the electronic communications of any alien abroad simply because the communications were acquired electronically in the

United States, even if none of the alien's communications were with a U.S. person. Such an overbroad application of the Fourth Amendment to foreign nationals abroad is unjustified. Nor is a warrant requirement necessary to protect the rights of U.S. persons, because Section 702 prohibits the targeting of a person abroad "if the purpose . . . is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2). Accordingly, no warrant requirement arises simply because surveillance of a foreign person located abroad was technologically effected in the United States.

2. Incidental Collection Does Not Trigger a Warrant Requirement

Muhtorov erroneously contends that the government needs a warrant to retain or use communications it acquires under Section 702 if a U.S. person is a party to those communications. But courts repeatedly have recognized that the incidental collection of third parties' communications that occurs as a result of constitutionally permissible acquisitions targeting others does not itself trigger a warrant requirement. *See Hasbajrami*, 945 F.3d at 663-64 (citing cases). This "incidental collection" principle is fully applicable in the Section 702 context. *See Mohamud,* 843 F.3d at 441 (holding that "because the target of the surveillance was a non-U.S. person located outside of the United States at the time of the surveillance, the government was not required to obtain a search warrant to collect" the email communications of a U.S. person with the foreign national "as

an incident to its lawful search of the foreign national's email" under Section 702); *Hasbajrami*, 945 F.3d at 664 (same); *United States v. Mohammad*, 339 F. Supp. 3d 724, 750-51 (N.D. Ohio 2018) (same); *see also In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008) (reaching a similar conclusion as to incidentally collected communications under the Protect America Act ("PAA"), a statute similar to Section 702 that expired in 2008).

Muhtorov argues (Br. 30-32) that the decisions establishing the incidental collection principle depend on the fact that a warrant had already been issued with respect to the target. But Muhtorov draws the wrong lesson from those cases. As the Ninth Circuit explained, those decisions involved searches "target[ing] United States citizens" conducted in the United States that themselves required "a warrant . . . for the initial search to be constitutionally permissible." *Mohamud*, 843 F.3d at 440. The key principle is that when surveillance is "lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful." *Hasbajrami*, 945 F.3d at 666 (internal quotation marks omitted). "The reason why the initial surveillance was lawful does not matter." *Id.*

3. The Foreign Intelligence Exception Applies

Alternatively, incidental collection under Section 702 falls within the foreign-intelligence exception to the warrant requirement. Neither the district court below nor the Second and Ninth Circuits addressed the foreign intelligence exception because those courts held that no warrant was required under *Verdugo-Urquidez* and the incidental collection doctrine. Nevertheless, the foreign-intelligence exception provides an independent basis for rejecting Muhtorov's contention that a warrant was required here.

Several courts of appeals have recognized, as a variant of the special needs exception, a foreign-intelligence exception to the warrant requirement. *See United States v. Duka*, 671 F.3d 329, 341 (3d Cir. 2011) (citing cases); *In re Directives*, 551 F.3d at 1010-12.[11] Foreign intelligence collection under Section 702 falls within that exception because the "programmatic purpose" of obtaining foreign intelligence information goes "beyond any garden-variety law enforcement objective," and "requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011.

[11] The only court of appeals to question the exception's application did so in the context of a "domestic organization" that was not "acting in collaboration with a foreign power." *See Zweibon v. Mitchell*, 516 F.2d 594, 614, 651 (D.C. Cir. 1975) (en banc) (plurality opinion).

Muhtorov incorrectly relies (Br. 35) on *In re Directives* in contending that the foreign intelligence exception applies only when the Attorney General finds probable cause that the target is a foreign agent. While *In re Directives* recognized that those requirements were appropriate for surveillance *targeting U.S. persons*, the court did not suggest that they are necessary for surveillance targeting *non-U.S. persons* abroad. *See In re Directives*, 551 F.3d at 1012. Indeed, the court upheld the PAA, even though it lacked those requirements for surveillance targeting foreign nationals abroad. *See id.* at 1015. Other courts have likewise held that the foreign intelligence exception applies in the Section 702 context. *See [Caption Redacted]*, 2011 WL 10945618, at *24 (FISC Oct. 3, 2011) ("*FISC 2011 Op.*"); *United States v. Mohamud*, 2014 WL 2866749, at *18 (D. Or. June 24, 2014); Opinion at 45-48, *United States v. Al-Jayab*, No. 1:16-cr-181 (N.D. Ill. Jun 28, 2018) (ECF No. 115) ("*Al-Jayab* Op.").

Finally, Muhtorov's reliance (Br. 34-35) on *United States v. United States District Court*, 407 U.S. 297 (1972) (*Keith*), is misplaced. The Court in *Keith* expressly reserved the issue of a warrant requirement for foreign intelligence collection. *Id.* at 308. Morevoer, *Keith* "implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible," *Clapper*, 568 U.S. at 402, and that rationale would apply *a fortiori* to

foreign intelligence surveillance under Section 702 targeted only at non-U.S. persons abroad.

D. The Section 702 Collection In this Case was Lawful under the Fourth Amendment's Reasonableness Test

Courts analyzing Section 702 collection have assumed that, "even absent a warrant requirement," the collection "must still be reasonable, at least insofar as it affects United States persons, to be consistent with the Fourth Amendment." *Hasbajrami*, 945 F.3d at 666. To determine whether a search is reasonable, the court "weigh[s] the promotion of legitimate governmental interests against the degree to which the search intrudes upon an individual's privacy." *Maryland v. King*, 569 U.S. 435, 448 (2013). Under the general reasonableness balancing test, warrantless searches are permissible where the government interest is especially strong or likely to be frustrated by the warrant requirement, where the search involves modest intrusions on individual privacy, and when safeguards restrain the government within reasonable limits. *See Illinois v. McArthur*, 531 U.S. 326, 330-31 (2001).

The Second and Ninth Circuits unanimously found that the Section 702 collection in those cases was reasonable under this test. *Mohamud*, 843 F.3d at 444 ("[e]ven assuming [the defendant] had a Fourth Amendment right in the incidentally collected communications, the search was reasonable.") *Hasbajrami*, 945 F.3d at 667 ("The incidental collection of communications between targeted

foreigners abroad and United States persons or persons in the United States is . . . reasonable"). This Court's review of the classified record will likewise support the conclusion that the government's acquisition and use of the Section 702 information in this case was reasonable, in light of the principles discussed below.[12]

1. Section 702 Collection Advances the Government's Compelling Interest in Obtaining Foreign Intelligence Information to Protect National Security

The government's national security interest in conducting surveillance under Section 702 to combat terrorism and other national security threats "is an urgent objective of the highest order." *Mohamud*, 843 F.3d at 441. *See also In re Directives*, 551 F.3d at 1012. In addition, the Privacy and Civil Liberties Oversight Board ("PCLOB") found that Section 702 is a uniquely valuable tool in the government's efforts to combat terrorism. PCLOB Report at 104-08. And the urgency of the government's interest is "greater, not less" when the foreign intelligence target communicates with associates in the United States. *Hasbajrami*,

[12] Muhtorov's challenge to the denial of his motion to suppress is necessarily limited to Section 702 as it was implemented in the specific searches or seizures that produced the evidence he seeks to suppress. *See Mohamud*, 843 F.3d at 438 & n.21 (defendant could not challenge Section 702 "techniques not employed in [his] particular case"). For that reason, Muhtorov's arguments related to "upstream" collection are not at issue in this case, which did not involve such collection. *See id.* (declining to consider "upstream[]" collection or other issues not involved in the case).

945 F.3d at 667; *see id.* ("If it is reasonable—and indeed necessary to the national security—for intelligence agencies to monitor the communications of suspected foreign terrorists abroad, the need to keep track of the potential threat from abroad does not lessen because some of the suspect's contacts turn out to be American nationals, or foreign nationals located within the United States").

Courts reviewing Section 702 collection have assumed that U.S. persons have at least some reasonable expectation of privacy in the contents of communications incidentally collected through targeting third parties abroad, while recognizing that such expectations may be diminished because U.S. persons have no cognizable interest in the accounts used by the foreign targets and have no control over their communications after they are sent. *See Mohamud*, 843 F.3d at 442; *see also United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (noting that individuals may lack "an expectation of privacy" in "e-mail(s) that have already arrived at the recipient") (quoting *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004)). Accordingly, those courts have uniformly recognized that the government's compelling interest in collecting foreign-intelligence information to protect the nation against terrorist threats outweighed the individual privacy interests of the U.S. persons whose communications were collected. *See, e.g.*, *Mohamud*, 843 F.3d at 441-44; *Hasbajrami*, 945 F.3d at 667; *Mohammad*, 339 F. Supp. 3d at 751-53. In reaching that conclusion, these courts have noted

that Section 702 surveillance is governed by stringent safeguards to ensure that it properly targets non-U.S. persons located outside the United States for foreign intelligence purposes, and to protect the privacy interests of U.S. persons.

2. The Privacy Interests of U.S. Persons Are Protected by Stringent Safeguards and Procedures

The government employs multiple safeguards that reasonably govern targeting decisions and the handling of U.S. persons' information that may be acquired.

a. Certification

Section 702 requires that the DNI and the Attorney General certify that procedures are in place to protect the privacy of U.S. persons. *See* 50 U.S.C. § 1881a(a), (h), and (j). The DNI and the Attorney General must also certify that a significant purpose of the acquisition is to obtain foreign intelligence information, that guidelines have been adopted to ensure compliance with the limitations in Section 702(b), and that the guidelines, targeting and minimization procedures are consistent with the Fourth Amendment. *See* 50 U.S.C. § 1881a(h)(2)(A). In requiring such high-level officials to oversee collection under Section 702, the statute helps ensure that Section 702 is appropriately used for important foreign-intelligence purposes.

b. FISC Review

The government's certification, targeting procedures, and minimization procedures are all subject to FISC review. *See* 50 U.S.C. § 1881a(j)(3)(A). Prior FISC approval further supports the conclusion that Section 702 collection conducted pursuant to such procedures is constitutional. *See Clapper,* 568 U.S. at 414 (noting the importance of the requirement that the FISC "assess whether the Government's targeting and minimization procedures comport with the Fourth Amendment").

The FISC subjects those procedures to exacting Fourth Amendment scrutiny. *See*, *e.g.*, *FISC 2008 Op.* at 32–40; *FISC 2011 Op.*, 2011 WL 10945618, at *5-6. In addition, "FISC review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather the Court also examines how the procedures have been and will be implemented." *[Caption Redacted]*, Mem. Op. at 3 (FISC Aug. 26, 2014) ("*FISC 2014 Op.*").[13]

c. Targeting procedures

Section 702 provides that targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United

[13] Available at https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf

States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). The FISC repeatedly has found that the targeting procedures meet that standard, and reviewing courts have agreed. *See Mohamud*, 843 F.3d at 443.

d. Minimization procedures

The government also employs FISC-approved minimization procedures to limit the acquisition, retention, and dissemination of information concerning U.S. persons, consistent with the government's foreign intelligence needs. *See* 50 U.S.C. § 1801(h)(1); PCLOB Report at 50 (The minimization procedures are "a set of controls on data to balance privacy and national security interests").[14] Minimization procedures limit how long information concerning U.S. persons can be retained and how it can be disseminated. The procedures require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. *See id.* at 64–65. As the FISC has held, the minimization

[14] The specific targeting and minimization procedures governing the collection in this case are classified, and are identified in the classified record.

procedures ensure that any intrusion on the privacy of U.S. persons is reasonably balanced against the government's intelligence needs. *See FISC 2008 Op*. at 40.

The Ninth Circuit found that the minimization procedures implemented in that case contributed to the reasonableness of the collection. *Mohamud*, 843 F.3d at 443-44 ("Based on our review of the classified record, we agree that the applicable targeting and minimization procedures, which were followed in practice, sufficiently protected Mohamud's privacy interest."); *see also In re Directives*, 551 F.3d at 1015 (finding it "significant" in upholding the PAA that "effective minimization procedures are in place" to "serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.").

Under Section 702, Congress and the Executive Branch have developed a balanced framework of court-approved procedures to enable foreign intelligence collection vital to the nation's security while protecting constitutionally protected privacy interests. *See In re Directives*, 551 F.3d at 1016 ("[W]here the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."). These safeguards ensured that the collection in this case targeted only foreign person(s) outside the United States and was conducted in a way that only incidentally implicated the

privacy of U.S. persons. Courts reviewing incidental collection under Section 702 in circumstances similar to this case have found that the government's actions were reasonable under the Fourth Amendment's balancing test. This Court should likewise hold that the government's Section 702 acquisition of foreign intelligence information in this case was reasonable.

3. Section 702 Collection Has Sufficient Particularity

Muhtorov misses the mark in arguing (Br. 38-40) that Section 702 collection is constitutionally unreasonable because it lacks the "core safeguards" of a particularized court order or probable cause finding. Section 702 collection is sufficiently focused and reasonable, given its foreign-intelligence context. The government must determine that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information and that the person uses a specific communications "selector," (such as an email address), and the government acquires only communications involving that particular selector. *See FISC 2011 Op.*, 2011 WL 10945618, at *7; PCLOB Report at 20-23, 32-33, 111-12.

Section 702 does not authorize bulk collection. *See 2014 FISC Op*. at 26 ("acquisitions are not conducted in a bulk or indiscriminate manner"); PCLOB Report at 103. Although particularity may be a factor in assessing reasonableness, the Fourth Amendment "imposes no irreducible requirement" of individualized

suspicion where the search is otherwise reasonable. *King*, 569 U.S. at 447 (citation omitted); *see also In re Directives*, 551 F.3d at 1013 (rejecting the petitioner's attempt to "reincorporate . . . the same warrant requirements" governing domestic surveillance that the court had "already . . . held inapplicable" to surveillance targeting foreigners abroad). While the number of communications intercepted by the government could be voluminous, the collection is neither indiscriminate nor untethered to a vital national security interest. Rather, Section 702's targeting procedures are sufficiently particularized for the purpose of the collection, and are thus reasonable under the Fourth Amendment. Indeed, with respect to this case, the district court found that the "[Section 702] surveillance at issue was narrowly tailored to the government's foreign intelligence-gathering prerogatives." Appellant's App. 119; *see also United States v. Hasbajrami*, 2017 WL 1029500, at *13 (E.D.N.Y. Mar. 8, 2016) (finding that the collection in that case "was as particular as it gets" because it involved "the targeting of specific non-U.S. persons outside the United States for specific counter-terrorism purposes"). This Court's review of the classified record will likewise show that the Section 702 collection here was appropriately "particular" and reasonable.

4. The Special Minimization Rules Under FISA § 1802 Do Not Apply

Muhtorov contends (Br. 43-44) that the post-collection warrant requirement he advocates is supported by a special provision of FISA, which generally

prohibits retention, without specific FISC approval, of U.S. persons' communications intercepted pursuant to surveillance of dedicated communications lines used exclusively by foreign powers (*e.g.*, foreign government hotlines). *See* 50 U.S.C. §§ 1801(h)(4), 1802(a)(1). Muhtorov's argument that the Fourth Amendment requires Section 702 surveillance to be governed by the same standards is illogical because the two provisions have fundamentally different purposes.

Surveillance under Section 1802 is subject to a strict minimization standard because it is limited to surveillance of communication lines that pose "no substantial likelihood" that U.S. persons will use them. *See* 50 U.S.C. § 1802(a)(1)(B). In contrast, Section 702 was enacted specifically to authorize surveillance of foreign intelligence targets, such as "foreign agents of terrorist organizations operating abroad," *Hasbajrami*, 945 F.3d at 666, and the foreign targets' communications "with persons inside the United States is thus of particular importance, and at least as important as monitoring the communications of foreign terrorists abroad among themselves." *Id*. at 667; *see also id.* at 665 ("That the overall practice of surveilling foreigners abroad of interest to the legitimate purpose of gathering foreign intelligence information may predictably lead to the interception of communications with United States persons no more invalidates that practice, or requires the government to cease its surveillance of the target until

a warrant is obtained, than the general foreseeability of intercepting communications with previously unknown co-conspirators undermines the inadvertent overhear doctrine in ordinary domestic criminal wiretapping."). Accordingly, "when the intelligence information properly collected raises reasonable grounds to believe that a crime is being committed or planned in the United States, dissemination of the information [without a warrant] to a domestic law enforcement agency such as the FBI is also reasonable." *Id.* at 667. Muhtorov's reliance on Section 1802 is nothing more than different packaging, under a purported "reasonableness" analysis, for his argument that a warrant is required when the government incidentally collects communications. As noted, courts have uniformly rejected that argument.

5. The Fourth Amendment Permits Queries Using Search Terms Associated with U.S. Persons Pursuant to Court-Approved Procedures

Muhtorov argues (Br. 40-50) that the minimization procedures are inadequate because, he claims, they permit the government to use Section 702 as a pretextual "back door" tool to amass a database of Americans' communications and query it using identities of U.S. persons for purposes unrelated to foreign intelligence. But the statute prohibits pretextual targeting of a person abroad if the purpose is to target a U.S. person or a person in the United States. *See* 50 U.S.C. § 1881a(b)(2). More generally, Muhtorov's argument relies on a mistaken premise

—that the Fourth Amendment requires judicial approval before the government may review communications it has already lawfully acquired under Section 702.

Contrary to Muhtorov's misleading label, a query of Section 702 information is not a "backdoor search." Querying does not result in the additional collection of any information. Rather, queries enable the government to efficiently locate foreign intelligence information, such as information related to a terrorist plot, without sifting through each individual communication. The minimization procedures appropriately restrict the government's ability to query Section 702 data using a query term associated with a U.S. person. *See generally* PCLOB Report at 56-58 (explaining that minimization procedures require that queries of Section 702-acquired information be designed so that they are "reasonably likely to return foreign intelligence information," or, in the case of the FBI, "evidence of a crime"); *id.* at 11 (noting that "procedures are in place to prevent queries being conducted for improper purposes").[15]

Such queries are not a new "search." They are simply a more efficient way for the government to focus on particular information within a larger set of lawfully-acquired communications that it is already authorized to review. Moreover, querying serves the government's compelling interests in detecting

[15] Section 702, as amended in 2018, now requires standalone querying procedures. *See* 50 U.S.C. § 1881a(f).

connections between persons in the United States and lawfully targeted foreign person who may be involved in perpetrating terrorist attacks or other national security threats. By helping agents and analysts to identify information that is likely related to threats, using queries can enhance privacy by reducing the need to review potentially sensitive information that is unlikely to be pertinent. The FISC has repeatedly found that the minimization rules governing the querying of Section 702 data satisfy statutory and constitutional requirements. *See, e.g.*, *[Caption Redacted]*, Memo. Op. 33-44 (FISC Nov. 6, 2015) ("*FISC 2015 Op.*").[16]

The Fourth Amendment does not require a judge to pre-approve queries of lawfully collected information. Such queries do not require a separate Fourth Amendment analysis, and permitting them, under the court-approved restrictions in

[16] Available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

In 2018, the FISC concluded that recent misapplications of the query standard by FBI personnel rendered the FBI's proposed 2018 minimization procedures deficient, as implemented, under FISA and the Fourth Amendment. *See [Redacted]*, 402 F. Supp. 3d. 45, 82-88 (FISC 2018), *aff'd on other grounds*, *In re DNI/AG 702(h) Certifications 2018 [Redacted]*, 941 F.3d 547 (FISA Ct. Rev. 2019). The FISC subsequently found that the FBI's revised procedures included additional safeguards that adequately addressed the deficiencies. *[Redacted]*, Memo. Op. 10-16 (FISC Sept. 4, 2019), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opinion_04Sep19.pdf. These FISC Opinions address the FBI's 2018 querying and minimization procedures but not the lawfulness of querying under earlier minimization procedures applicable in this case.

the minimization procedures, does not make Section 702 surveillance unreasonable under the Fourth Amendment. *See id*. at 40.

That conclusion is consistent with well-established Fourth Amendment principles. Courts have held in various contexts that the government's querying of information that it has already lawfully obtained does not implicate any reasonable expectation of privacy beyond that implicated in the initial collection. *See, e.g.*, *Boroian v. Mueller*, 616 F.3d 60, 67-68 (1st Cir. 2010) ("[T]he government's retention and matching of [an individual's] profile against other profiles in [a DNA database] does not violate a [reasonable] expectation of privacy . . . and thus does not constitute a separate search under the Fourth Amendment."); *see also Johnson v. Quander*, 440 F.3d 489, 498-99 (D.C. Cir. 2006) ("[A]ccessing the records stored in [a DNA] database is not a 'search' for Fourth Amendment purposes"). That is true even when the query's purpose is different from the purpose of the original collection. *See, e.g.*, *King*, 569 U.S. at 465 (upholding warrantless collection of DNA for identification of persons arrested for serious offenses and subsequent use of DNA in prosecution of unrelated, unsolved crimes); *Jabara v. Webster*, 691 F.2d 272, 279 (6th Cir. 1982) (upholding dissemination by NSA of intelligence collected without a warrant for intelligence purposes to FBI for purposes of criminal investigation).

The Second Circuit in *Hasbajrami* departed from this analysis, stating that querying Section 702 data using search terms associated with the defendant could constitute "a separate Fourth Amendment event that, in itself, must be reasonable," 945 F.3d at 670.[17] For the reasons set forth above, the Second Circuit erred in concluding that Section 702 queries amount to a separate "search" requiring an independent reasonableness analysis beyond the restrictions in the minimization procedures. *See [Redacted]*, 402 F. Supp. 3d. at 86 (rejecting amici's argument that each query is "a distinct Fourth Amendment event"); *FISC 2015 Op.* at 40 (same). The Second Circuit relied on cases holding that, in some contexts, the government may need "additional probable cause or reasonableness assessments to support a search of information or objects" the government had lawfully seized in an initial search. *Hasbajrami*, 945 F.3d at 670. But that "additional" reasonableness assessment was required in those cases because the government obtained information that was beyond the scope of the original warrant or warrant exception. *See, e.g.*, *Riley v. California*, 573 U.S. 373 (2014) (holding that officers generally require a warrant to search digital data in a cellular phone under the search-incident-to-arrest doctrine, because such searches go beyond the officer-safety and evidence-preservation rationales of the doctrine); *United States v.*

[17] The court remanded for a determination whether any querying related to the defendant's suppression motion was reasonable. 945 F.3d at 676-77.

Sedaghaty, 728 F.3d 885, 912-13 (9th Cir. 2013) (invalidating government seizure of evidence related to terrorism obtained from the defendant's computer pursuant to a warrant expressly limited in scope to evidence related to tax violations). Those cases do not apply to querying communications lawfully acquired under Section 702 because the government is already authorized to review them for proper purposes under court-approved minimization procedures. *See FISC 2015 Op.* at 40; *see also United States v. Lustig*, 830 F.3d 1075, 1085 (9th Cir. 2016) (recognizing the general rule that "once an item has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant"). The queries permitted by those procedures fall within the purpose and scope of the collection as authorized by Congress and the FISC.

As the FISC has held, the minimization procedures reasonably protect the privacy interests implicated by querying using U.S. person identifiers, balanced against the government's compelling foreign-intelligence interest in conducting such queries. In light of those procedures, there is no constitutional requirement of prior judicial review or other additional Fourth Amendment analysis of each individual query. The FISC-approved minimization procedures permit the government to review the information it lawfully collects under Section 702, which includes information concerning U.S. persons, to assess whether the information

should be retained or disseminated. Accordingly, U.S. person information is by necessity already subject to review (and use) under those procedures. Under Section 702, the collection and communication-by-communication review of information is lawful under the Fourth Amendment, and there is no basis to require additional judicial process for the more focused review of the same information in response to tailored queries.

In any event, this Court's reasonableness analysis should focus on the way the government used the Section 702 information at issue in this case. *See Mohamud*, 843 F.3d at 438 n.21 (explaining that a court may not "suppress evidence based on a Fourth Amendment challenge to techniques not employed in a particular case"). As the district court found, the government's use of Section 702 authority in this case was reasonable and fully compliant with the governing statute and procedures. "[T]he [Section 702] surveillance at issue was narrowly tailored to the Government's foreign intelligence-gathering prerogatives, and once [the government] identified [Muhtorov] as a U.S. person on U.S. soil . . . authority to target him directly was specifically and timely sought." Appellant's App. 266.

Muhtorov and amici express concern that the government may conduct "back-door," fishing-expedition queries of Section 702 data to bolster investigations of ordinary, domestic crimes. But this case—a terrorism prosecution where the defendant tried to join a foreign terrorist organization

fighting against U.S. forces overseas after communicating directly with that organization for years—does not implicate those concerns. The classified record shows that this case did not arise from any exploitation of Section 702 information beyond the original foreign-intelligence purpose of the collection. The government's use of Section 702 information in this case was fully consistent with the Fourth Amendment.

Even if queries of lawfully obtained information may constitute a separate search, this Court's analysis should be limited to alleged "searches" where a causal link can be drawn between the search and the acquisition of evidence used against Muhtorov. Both FISA and the Fourth Amendment provide a suppression remedy only when the government seeks to introduce evidence that was obtained or derived from the challenged search. *See* 50 U.S.C. § 1806(c), (e); *id.* § 1881e(a); *see also Murray v. United States*, 487 U.S. 533, 536-37 (1988) (suppression is available only when the acquisition of evidence that the government intends to introduce at trial was a direct or indirect result of an unlawful search); *Mohamud*, 843 F.3d at 438 & n.21 (limiting the defendant's challenge to the specific Section 702 techniques that resulted in the specific emails that were used to obtain a FISA warrant). In this case, the classified record shows that the Section 702-derived evidence at issue was not obtained or derived from queries using terms associated with Muhtorov. Accordingly, this Court, like the Ninth Circuit in *Mohamud*, can

decide this case without addressing the merits of Muhtorov's challenge to the use of such queries. *See Mohamud*, 843 F.3d at 442.

E. The FISC's Role in Reviewing Section 702 Procedures is Consistent with Article III

Muhtorov argues (Br. 47-51) that the FISC's role in approving the government's Section 702 procedures violates Article III's case-or-controversy requirement because the court does not review the procedures in the context of a particular proposed target. That contention has no merit, as the Ninth Circuit unanimously held. *See Mohamud*, 843 F.3d at 444 n.28. Every district court to consider similar Article III challenges has likewise rejected them. *See* Appellant's App. 133-37; *Mohamud*, 2014 WL 2866749, at *11; *Al-Jayab Op*. at 56-58.

"Article III courts perform a variety of functions not necessarily or directly connected to adversarial proceedings in a trial or appellate court." *Mistretta v. United States*, 488 U.S. 361, 389 n.16 (1989). In particular, courts have long participated in overseeing government searches by reviewing warrant and wiretap applications, notwithstanding that these proceedings are wholly ex parte and do not involve an aggrieved party as ordinarily required for a "case or controversy" under Article III. *See id.* at 389 n.16; *see also, e.g.*, *In re Sealed Case*, 310 F.3d 717, 732 n.19 (FISA Ct. Rev. 2002) ("[W]e do not think there is much left [after *Mistretta*] to an argument . . . that the statutory responsibilities of the FISA court are inconsistent with Article III.").

Congress assigned the FISC an analogous function in Section 702 that is entirely consistent with the traditional function of Article III courts in protecting the privacy rights of persons whose interests are potentially implicated by proposed searches, seizures, or compulsory processes. As the Ninth Circuit explained in rejecting the same Article III arguments that Muhtorov raises here, the FISC's "review of § 702 surveillance applications . . . is [as] central to the mission of the judiciary as it is similar to the review of search warrants and wiretap applications." *Mohamud*, 843 F.3d at 444 n.28 (citing *Mistretta*, 488 U.S. at 388) (internal quotation marks omitted).

Muhtorov is also incorrect in arguing (Br. 49) that the FISC's review of Section 702 procedures is unconstitutional because it lacks a "concrete factual context relating to particular targets." Even the authority Muhtorov relies on recognizes that the standard is whether the questions presented to the FISC "are in a form such that a judge is capable of acting on them." *United States v. Megahey*, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982). That standard is met here.

The Article III judges on the FISC are fully capable of reviewing specific targeting and minimization procedures to determine whether they comply with applicable statutory standards and the Fourth Amendment. Courts regularly undertake that kind of analysis when they adjudicate the facial constitutionality of statutes regulating searches and seizures. *See City of Los Angeles v. Patel*, 135 S.

Ct. 2443, 2450 (2015). Moreover, the FISC reviews the procedures "in light of the purpose and technique of the particular surveillance." 50 U.S.C. § 1801(h); *see id.* § 1821(4)(A). The FISC closely considers how detailed procedures apply to specific, technical tools through which the government implements Section 702. *See*, *e.g.*, *FISC 2011 Op.*, 2011 WL 10945618, at *9. In sum, although warrant or wiretap applications for law enforcement purposes typically involve a more fact-specific form of review, that is because the Fourth Amendment or Title III requires more particularity in those contexts—not because of any requirements in Article III.[18]

Finally, even if the FISC's role were somehow improper, Muhtorov has not explained how the FISC's participation violated *his* rights or would provide a basis for excluding evidence. Section 702 surveillance results from directives authorized by Section 702 itself, not from the FISC's review of the government's procedures. The effect of that review is to protect the rights of individuals such as Muhtorov, whose communications may be incidentally collected. *See Mohamud*, 2014 WL 2866749, at *11 ("FISC review of § 702 surveillance submissions provides prior review by a neutral and detached magistrate [which] strengthens, not undermines, Fourth Amendment rights.").

[18] To the extent Muhtorov contends (Br. 49) that the FISC's orders are "advisory" opinions, he is incorrect. *See Mohamud*, 2014 WL 2866749, at *11.

F. The Good Faith Exception to the Exclusionary Rule Applies

The good-faith exception to the exclusionary rule provides an independent basis to uphold the government's actions in Muhtorov's case. *See United States v. Leon*, 468 U.S. 897, 913 (1984); *see also Davis v. United States*, 564 U.S. 229, 236-39 (2011). The good-faith rule applies, among other times, when law enforcement agents act in "objectively reasonable reliance on a statute." *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987). The good-faith exception applies here because government agents relied on the fruits of surveillance that was conducted pursuant to Section 702, consistent with the procedures approved by the FISC, which was objectively reasonable under the circumstances.

II. The District Court Properly Withheld the FISA Materials from Defense Counsel

The district court did not abuse its discretion in denying Muhtorov's motion for disclosure of classified FISA materials.

When a defendant moves to suppress FISA evidence, the government may file a declaration from the Attorney General stating that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). If the Attorney General files such a declaration, as he did here, the district court must review the FISA materials ex parte and in camera and may order disclosure of those materials "only where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance." *Id.* (emphasis

added); *see also id.* § 1881e(a) (providing that this same procedure governs motions to suppress Section 702-related information). A court may order disclosure only if it finds that it cannot accurately resolve the lawfulness of the collection. *See United States v. Daoud*, 755 F.3d 479, 481-83 (7th Cir. 2014). Courts have consistently held that "[d]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule." *United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011).

Here, the in camera, ex parte review the district court conducted in this case was the appropriate method to determine whether the Section 702 collection was lawful. Every other court that has reviewed the lawfulness of Section 702 collection has done the same. *See Mohamud*, 2014 WL 2866749, at *32; *United States v. Hasbajrami*, 2016 WL 1029500, at *14; *Mohammmad*, 339 F. Supp. 3d at 756-57; *Al-Jayab Op*. at 71-75. This Court should likewise review the classified materials and reach the same conclusion. *See United States v. Mohamud*, 666 F. App'x 591, 597 (9th Cir. 2016) ("The district court did not abuse its discretion by denying Mohamud's security-cleared counsel access to classified [FISA and Section 702] materials."); *Daoud*, 755 F.3d at 485 ("[o]ur own study of the classified materials has convinced us . . . that their disclosure to the defendant's lawyers is . . . not 'necessary'").

Muhtorov's contention that this Court should order disclosure of the FISA materials due to the novelty and complexity of the issues he has raised is inconsistent with all of those cases, and with the statutory standard. When FISA was enacted, every FISA suppression motion would have raised "novel" issues, yet Congress mandated that FISA litigation be handled ex parte and in camera, with disclosure being the exception. Courts have uniformly followed that procedure for decades. *See, e.g.*, *El-Mezain*, 664 F.3d at 567. Moreover, the statute requires that courts review FISA applications and orders in camera and ex parte first, and only then determine whether disclosure is necessary. A court's decision to disclose should arise from that review, rooted in facts from the FISA materials, and not from a defendant's assertion that the issues he raises are novel and complex. *See Daoud*, 755 F.3d at 481-82; *see also United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) (rejecting defendant's argument that the legality of FISA surveillance was "too complex" to be resolved without disclosure and adversary proceedings).

III. Muhtorov Is Not Entitled to Disclosures About Other Techniques that He Speculates the Government Might Have Used In its Investigation

In a separate disclosure claim, Muhtorov speculates (*see* Br. 72-75) that the government might have used investigative tools other than traditional FISA and Section 702 in his case, such as: (1) the overseas acquisition of information

pursuant to E.O. 12,333[19] (2) the collection of location tracking information; and (3) the acquisition of telephone call detail records through a now-defunct program involving NSA's acquisition of non-content telephone metadata pursuant to Section 501 of FISA, 50 U.S.C. § 1861.[20] Muhtorov contends (Br. 76) that the district court erred in denying his request for the disclosure of: (1) each surveillance technique the government used to obtain information about his communications or activities; (2) the timing or duration of each technique; (3) the legal authority the government relied upon; and (4) the evidence obtained or derived from each surveillance technique.

The district court correctly rejected this claim. *See* ROA Vol. 13 at 716. Every court to have considered a similar claim has likewise rejected it. *See*, *e.g.*, *Mohammad*, 339 F. Supp. 3d at 753-59. There is no reason for this Court to reach a different result.

---

[19] *See* Part I.B.1, *supra*.

[20] From 2006 to 2015, NSA obtained telephony metadata, or "call detail records," in bulk from U.S. telecommunications service providers to use in counterterrorism investigations pursuant to FISC orders issued under FISA's "business records" provision. The records acquired included information about calls, such as the numbers of incoming and outgoing calls and the times calls were placed, but it did *not* include the contents of calls, the names of callers, or cell-site location information. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things*, 2013 WL 5741573, at *1 (FISC Aug. 29, 2013).

A. Standards of Review

This Court reviews the district court's discovery rulings, including rulings pursuant to the Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3, for an abuse of discretion. *E.g.*, *United States v. Bowers*, 847 F.3d 1280, 1291 (10th Cir. 2017); *United States v. Lustyik*, 833 F.3d 1263, 1271 (10th Cir. 2016). This Court reviews questions of constitutional and statutory interpretation *de novo*. *United States v. Sorensen*, 801 F.3d 1217, 1225 (10th Cir. 2015).

B. The Government's Discovery and Disclosure Obligations Do Not Extend to the Additional Information Demanded by Muhtorov

Discovery in criminal cases is "rather limited." *See*, *e.g.*, *Degen v. United States*, 517 U.S. 820, 825 (1996). There is no rule generally requiring the government to provide a criminal defendant with information concerning the origins of the investigation that led to his arrest. *See Pennsylvania v. Ritchie*, 480 U.S. 39, 59 (1987) (a "defendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the [government's] files"). Rather, the government's disclosure obligations are generally established by the Federal Rules of Criminal Procedure, the Jencks Act, and *Brady v. Maryland*, 373 U.S. 83, 87 (1963). Neither these authorities, nor any other authority identified by Muhtorov, requires the disclosures that he demands.

1. The Disclosures Demanded by Muhtorov Are Not Required by the Constitution

a. Muhtorov's principal contention is that "[d]ue process requires notice of surreptitious electronic surveillance in criminal cases because meaningful challenges are impossible without it." Br. 70. But none of the decisions that he cites (*see* Br. 76-78, 85-86) supports that contention or otherwise establishes that the district court was required to grant his demand for disclosures. That is especially true here, where the government specifically notified Muhtorov of traditional FISA and Section 702 surveillance and specifically denied that any evidence was derived from surveillance under E.O. 12,333. The district court was within its discretion to deny Muhtorov's speculative demands for additional notice.

Muhtorov's reliance on *Alderman v. United States*, 394 U.S. 165 (1969), is misplaced. In *Alderman*, the Supreme Court held that voluminous transcripts of conversations that had been illegally recorded should be disclosed to the defense because the task of determining whether any of those records "might have contributed to the Government's case" as to a particular defendant was "too complex" for the district court's in camera review. *Id.* at 182. *Alderman* is distinguishable because it involved (1) an acknowledged violation of constitutional rights; (2) multiple defendants whose separate rights could not be adequately protected by in camera review; and (3) a concession by the government that the surveillance was illegal and the fruits of the surveillance was arguably relevant in

determining the defendants' guilt. *Id.* at 184. None of those factors is present here.[21]

Keith is equally unhelpful to Muhtorov. In *Keith*, the Supreme Court held that the Fourth Amendment required the government to obtain judicial approval before conducting electronic surveillance for the purpose of domestic security. 407 U.S. at 323-24. The Court concluded that, because the surveillance in question was unlawful, the government was required under *Alderman* to disclose the impermissibly intercepted conversations to the defendant. *Id.* at 324. But, as in *Alderman*, the Court did not state or suggest that a defendant has a broad right to disclosure of each surveillance technique used by the government, absent any established or admitted illegality. *See also id.* at 321-22 & n.20 (emphasizing that the Court did not reach the Fourth Amendment considerations associated with foreign intelligence surveillance.).

Jencks v. United States, 353 U.S. 657 (1957), *Berger v. New York*, 388 U.S. 41, 60 (1967), and *Dalia v United States*, 441 U.S. 238 (1979), also fail to support Muhtorov's demand for disclosures. Nowhere in those cases did the Supreme Court establish a right to disclosure of each surveillance technique used by the

[21] Muhtorov cites two other opinions from the same case, *Kolod v. United States*, 390 U.S. 136 (1968) (per curiam), and *United States v. Alderisio*, 424 F.2d 20 (10th Cir. 1970). But neither recognizes anything approaching the broad right to disclosure that he asserts.

government. Nor did the Court have occasion in any of these cases to address the distinct Fourth Amendment considerations associated with foreign intelligence surveillance.

b. Muhtorov cites two additional, more recent decisions that he claims "show that notice and adversarial litigation of Fourth Amendment questions [are] essential in an era of rapidly advancing technology." Br. 76. But neither of those decisions supports his claim.

In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Supreme Court held that the government's acquisition from a service provider, during a criminal investigation, of seven or more days of historical cell-site location records is a Fourth Amendment "search" generally subject to the warrant requirement. *Id.* at 2217. The Court did not address whether or in what circumstances the government must provide notice or other information to a criminal defendant concerning its acquisition of cell-site location records or of other investigative techniques. Moreover, the Court emphasized that its decision was "narrow" and that it "[was] not express[ing] a view on matters not before [it]," including, among other things, "collection techniques involving foreign affairs or national security." *Id.* at 2220.

Muhtorov does not identify any location data that was introduced at trial, nor does he identify any disputed issue relevant to determining his guilt that depended on where he was at a particular moment. Moreover, Muhtorov would not be

entitled to suppression of location data even if the government had introduced any, because, before *Carpenter*, obtaining such data from third parties without a warrant was lawful. *See United States v. Thompson*, 866 F.3d 1149, 1156-58 (10th Cir. 2017) (holding, based on *Smith v. Maryland*, 442 U.S. 735 (1979), that "[cell-site location information] is not protected by the Fourth Amendment"), *overruled,* 740 F. App'x 166 (2018) (unpublished); *see also Davis*, 564 U.S. at 241 (exclusionary rule does not apply to search conducted in reasonable reliance on binding precedent).

American Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015), is equally unhelpful to Muhtorov. There, the Second Circuit held in a civil case that NSA's bulk collection of non-content call detail records was not authorized by the FISA business records provision under which the FISC had approved it. *See id.* at 821. The Second Circuit declined to reach the plaintiffs' constitutional challenges, *see id.* at 825, and it did not address whether or in what circumstances the Constitution requires the government to notify a criminal defendant of the investigative techniques it has used. To the extent that *Clapper* sheds any light on such questions, it demonstrates that parties can effectively litigate legal challenges to intelligence-collection programs without the sort of detailed information that Muhtorov demands. *See id.* at 800-01. Moroever, *Clapper* notwithstanding, Muhtorov would not have been entitled to the suppression of call detail records

obtained through the NSA program, even if the government had introduced any, because any such records would have been acquired in good faith reliance on a FISC order. *See Leon*, 468 U.S. at 913.

2. Fed. R. Crim. P. 16 Does Not Support Muhtorov's Demand

Muhtorov contends that the government was required under Rule 16(a)(1)(B) and 16(a)(1)(E) to provide him with disclosures concerning the government's surveillance techniques, which he claims are "essential to [his] ability to seek suppression." Br. 80. That contention lacks merit.

Rule 16(a)(1)(B) provides for the disclosure by the government of the defendant's "written or recorded statement[s]" that are relevant. Nothing in this provision requires the government to make disclosures to a defendant about the investigative tools that it has used in building its case. The government fully complied with Rule 16(a)(1)(B) by providing Muhtorov, in discovery, with the substance of his relevant written or recorded statements.

Rule 16(a)(1)(E) also fails to support Muhtorov's claim for surveillance-related disclosures. It states in pertinent part that the government must permit the defendant to inspect and copy documents or other items if they are "within the government's possession, custody, or control" and are either "material to preparing the defense" or were "obtained from or belong[] to the defendant." Fed. R. Crim. P. 16(a)(1)(E). Contrary to Muhtorov's contention (Br. 80), it is self-evident that

information about the means used to investigate him does not "belong[] to [him]." Nor has Muhtorov made an adequate showing that the government is in possession of any item that is "material to preparing the defense."

Establishing materiality requires "facts which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995). "Neither a general description of the information sought nor conclusory allegations of materiality suffice." *Id.* Moreover, it is well settled that Rule 16 does not authorize "a blanket request to see the prosecution's file" or a "'fishing expedition'" by the defense. *United States v. Maranzino*, 860 F.2d 981, 985-86 (10th Cir. 1988) (citation omitted).

Muhtorov falls far short of meeting Rule 16's materiality standard. He merely speculates that the government might have engaged in various kinds of surveillance and might have information about such purported surveillance. Such speculative and conclusory allegations amount to the sort of fishing expedition that this Court and other courts have found to be insufficient to support a claim under Rule 16(a)(1)(E). *See*, *e.g.*, *United States v. Simpson*, 845 F.3d 1039, 1056 (10th Cir. 2017); *United States v. Spagnuolo*, 549 F.2d 705, 712-13 (9th Cir. 1977); *Santiago*, 46 F.3d at 894-95. The district court acted well within its discretion

under Rule 16(a)(1)(E) in denying Muhtorov's demand. *See Mohammad*, 339 F. Supp. 3d at 758-59 (rejecting similar claim).[22]

3. Muhtorov Is Not Entitled to Relief Under 18 U.S.C. § 3504

Muhtorov's claim (Br. 79) that the disclosures he seeks are required by 18 U.S.C. § 3504 also lacks merit. Section 3504(a) provides in relevant part that "[i]n any . . . proceeding," in response to "a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act," the government "shall affirm or deny the occurrence of the alleged unlawful act." The term "unlawful act" is defined (subject to certain exceptions) to include using a "device" (as defined in 18 U.S.C. § 2510(5)) to intercept the contents of "a wire, oral, or electronic communication," when such interception violates federal law. 18 U.S.C. § 3504(b); *id*. § 2510(5).

Two of the three forms of possible "surveillance" that Muhtorov identifies (Br. 72-76)—the acquisition of non-content call detail records and location tracking information—clearly fall outside the reach of Section 3504. Section 3504 applies only when an aggrieved party alleges that the government seeks to admit

[22] The single Rule 16(a)(1)(E) decision cited by Muhtorov did not involve the sort of speculation at issue here and is distinguishable. In *United States v. Soto-Zuniga*, 837 F.3d 992 (9th Cir. 2016), it was undisputed that the defendant had been arrested at an immigration checkpoint and that the government possessed the records that he sought to challenge his arrest. *Id.* at 1000–02.

evidence that is the product of an "unlawful act"—*i.e.*, the illegal use of a "device" capable of intercepting the contents of communications. *Id.* § 3504(b) (incorporating 18 U.S.C. § 2510(5)); *see* 18 U.S.C. § 2510(4) (defining "intercept," as used in § 2510, to mean "the aural or other acquisition of the *contents* of any wire, electronic, or oral communication") (emphasis added); *id.* § 2510(8) (defining "contents"). Neither the collection of call detail records nor the acquisition of location data such as cell-site location information involves the use of a device to acquire the contents of communications. Accordingly, Section 3504 does not apply to them.

Moreover, Muhtorov failed to make the necessary showing to require a response from the government under Section 3504. Muhtorov offered nothing beyond general speculation that the government engaged in unlawful surveillance of him. *See* Br. 72-73. Because Muhtorov failed to make a colorable claim that evidence in his case was inadmissible on the ground that it was the primary product of an unlawful act as to which he was aggrieved, the government was not required to affirm or deny the occurrence of any such allegedly unlawful act. *See*, *e.g.*, *United States v. Robins*, 978 F.2d 881, 886 (5th Cir. 1992) ("[A] motion alleging only a 'suspicion' of such surveillance, or that the movant has 'reason to

believe' that someone has eavesdropped on his conversations, does not constitute a positive representation giving rise to the government's obligation to respond.").

The only Section 3504 case Muhtorov cites (Br. 79), *United States v. Apple*, 915 F.2d 899 (4th Cir. 1990), undermines his claim. In *Apple*, the Fourth Circuit held that one defendant, Sherrie, had made a colorable showing that she was "aggrieved" by the surveillance at issue (a state wiretap on an alleged accomplice's phone), where there was "never . . . any question" the allegedly unlawful surveillance in fact occurred, and therefore the government had to respond to Sherrie pursuant to Section 3504. *Id.* at 907. Sherrie had submitted an affidavit identifying a specific conversation she had on the tapped line during the period in which it was tapped. *See id.* By contrast, the Fourth Circuit held that Section 3504 required no government response as to another defendant, Stacy, who had offered "mere suspicion" that his communications had been intercepted on the tapped line. *Id.* Muhtorov's claim falls far short of Sherrie's specific claim and is even weaker than the unsuccessful claim made by Stacy, who could at least point to a particular allegedly unlawful wiretap. Muhtorov's claim, by contrast, is pure conjecture.

Finally, the government provided the defense and the district court with a denial that satisfies Section 3504 with respect to Muhtorov's speculation that his communications were acquired under E.O. 12,333. The government stated:

> Assuming arguendo that § 3504 applies to surveillance conducted pursuant to Executive Order 12,333, and that the defendants have

> provided a colorable basis to believe they were surveilled, the government denies 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. The government will provide any additional information regarding this issue to the Court *ex parte*.

ROA Vol. 5 at 205. Assuming Muhtorov was entitled to a response at all, the government's denial was more than adequate given the speculative nature of Muhtorov's assertions. *United States v. Alvillar*, 575 F.2d 1316, 1321 (10th Cir. 1978) (holding that an informal denial of surveillance suffices where the defendant's allegations are "conclusory" and "unsupported").

Contrary to Muhtorov's contention (*see* Br. 80 n.37), the government's response (again, assuming one was required) was properly limited to denying that any evidence at trial was the product of allegedly unlawful surveillance pursuant to E.O. 12,333. Section 3504 requires a direct connection between a defendant's claim that unlawful surveillance occurred and the evidence to be admitted at trial. By its terms, Section 3504 applies "upon a claim by a party aggrieved that *evidence is inadmissible* because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act." 18 U.S.C. § 3504(a)(1) (emphasis added); *see also United States v. Shelton*, 30 F.3d 702, 707 (6th Cir. 1994) ("Section 3504 comes into play only on a claim that evidence is inadmissible."). Thus, a defendant cannot merely "seek[] disclosure of illegal

electronic surveillance . . . to learn when the government became interested in him as a target for investigation." *Robins*, 978 F.2d at 887.

C. The District Court Did Not Abuse its Discretion in Conducting Ex Parte Proceedings Under FISA and CIPA

1. To the extent that Muhtorov claims (*see* Br. 71) he is entitled to the disclosure of any portions of the FISA materials discussed above that might describe the use of other investigative tools, his claim amounts to an attempt to circumvent FISA and must be rejected. As discussed above, when the government intends to use against an aggrieved person at trial information obtained or derived from traditional FISA or Section 702, FISA requires the government to "notify the aggrieved person . . . that the [g]overnment intends to so disclose or so use such information." 50 U.S.C. § 1806(c); *see id.* §§ 1825(d), 1881e. The government provided Muhtorov such notice before trial, enabling him to move to suppress. As discussed above, *see* Part. II, the district court properly concluded, following an in camera, ex parte review as provided by FISA, that the FISA collection was lawfully authorized and conducted. Accordingly, FISA precludes disclosing to the defense any information contained in the FISA materials, including the facts establishing probable cause and any details about the manner in which those facts were obtained. *Id.*

2. Muhtorov claims (Br. 81-88) that the district court improperly relied on

CIPA in refusing to disclose the requested information about its surveillance techniques. Muhtorov does not seek this Court's review of all the district court's CIPA orders—his claim is limited to CIPA rulings, if any, concerning information that would support an additional motion to suppress evidence derived from "novel surveillance techniques." Br. 81 Even assuming arguendo that some of the classified information that was the subject of the CIPA rulings involved surveillance techniques as to which Muhtorov demands disclosures, his challenge to those rulings lacks merit.

CIPA governs how federal courts address matters concerning the discovery, admissibility, and use of classified information in criminal cases. *See United States v. Apperson*, 441 F.3d 1162, 1192-93 & n.8 (10th Cir. 2006); *Sedaghaty*, 728 F.3d at 904-05. CIPA "establish[es] procedures to harmonize a defendant's right to obtain and present exculpatory material upon his trial and the government's right to protect classified material in the national interest." *United States v. Abu-Jihaad*, 630 F.3d 102, 140 (2d Cir. 2010) (citation and quotation marks omitted). "[CIPA] is a procedural statute, however, that does not give rise to an independent right to discovery." *Lustyik*, 833 F.3d at 1271.

In this case, the district court granted several government motions under CIPA Section 4. Section 4 provides that, where classified information is potentially subject to discovery, the court "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." 18 U.S.C. app. 3 § 4; *see United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988). "CIPA does not itself create a government privilege against the disclosure of classified information; it presupposes one." *United States v. Hanna*, 661 F.3d 271, 295 (6th Cir. 2011). "Section 4 allows the government to for[]go presenting certain evidence to the defendant 'upon a sufficient showing.'" *Id.* (quoting 18 U.S.C. app. 3 § 4).

The government makes the "sufficient showing" required to delete materials from discovery under Section 4 by demonstrating that the materials in question are not "relevant and helpful" to the defense under the standard of *Roviaro v. United States*, 353 U.S. 53 (1957). *See*, *e.g.*, *United States v. Amawi*, 695 F.3d 457, 469-70 (6th Cir. 2012). Under that standard, the court must first determine whether the information is relevant, and, if so, whether the government's assertion of privilege is at least colorable. *Id*. Then, because classified information is not discoverable on a mere showing of theoretical relevance, the court determines whether the information satisfies the higher bar of being "relevant and helpful" under *Roviaro*. *Id.* If classified information does not satisfy this standard, the government may withhold it from discovery. *See id.*

Contrary to Muhtorov's apparent belief (*see* Br. 84), even when classified information has been found to satisfy the "relevant and helpful" standard, it is not necessarily subject to discovery. Instead, CIPA Section 4 expressly contemplates alternatives pursuant to which the government may "substitute a summary of the information for such classified documents" or "substitute a statement admitting relevant facts that the classified information would tend to prove." 18 U.S.C. app. 3 § 4. Such a substitution must "provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information." *See id.* § 6(c)(1).[23]

CIPA explicitly authorizes ex parte proceedings when the government submits materials to the district court for the court to determine whether they must be disclosed to the defense. Section 4 provides that the court may permit the government to make a request to delete classified materials from discovery "in the form of a written statement to be inspected by the court alone." 18 U.S.C. app. 3 § 4; *see also* Fed. R. Crim. P. 16(d)(1) ("The court may permit a party to show good cause [for an order restricting discovery] by a written statement that the court will inspect ex parte."). The courts of appeals have uniformly upheld ex parte proceedings under CIPA Section 4. *See United States v. Asgari*, 940 F.3d 188,

[23] Additionally, overriding national security concerns may, on balance, trump the defendant's need for the information that has been found to be relevant and helpful. *See Sarkissian*, 841 F.2d at 965.

191-92 (6th Cir. 2019) (reversing order requiring the disclosure of classified materials to security-cleared defense counsel for the purpose of aiding district court's determination whether the information was relevant and helpful to the defense); *see also*, *e.g.*, *Sedaghaty*, 728 F.3d at 904-05; *United States v. Mejia*, 448 F.3d 436, 457-58 (D.C. Cir. 2006); *United States v. Pringle*, 751 F.2d 419, 427-28 (1st Cir. 1984).

In conducting ex parte review under CIPA Section 4, the district court acts, in essence, as "standby counsel for the defendants," placing itself in defense counsel's shoes and determining what may be relevant and helpful to their case. *Amawi*, 695 F.3d at 471; *see also Asgari*, 940 F.3d at 191. To aid that review, the court may (but need not) also receive ex parte presentations from the defense explaining its theory of the case and the kinds of materials that would be helpful. *See*, *e.g.*, *Amawi*, 695 F.3d at 472.

Contrary to Muhtorov's contention, the district court correctly applied CIPA here. As this Court's review of the classified record will confirm, the district court properly applied the three-part test to determine that: (1) the classified materials that the government proposed to withhold from discovery were not "relevant and helpful" to the defense; and (2) the substitutions for classified information offered by the government would "provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified

information." *See* 18 U.S.C. app. 3 § 6(c)(1). This Court's review will also confirm that the district court closely scrutinized the government's classified submissions and steadfastly protected Muhtorov's interests. More than once, the district court revisited earlier CIPA rulings based on developments in the case and required the government to make additional disclosures to the defense or to provide additional facts and analysis to justify continuing to withhold information from discovery. *See* ROA Vol. 7 at 16-17 (discussing CIPA proceedings).

Muhtorov is incorrect in asserting (Br. 84) that the district court misapplied CIPA because the disclosures he demands are "discoverable and per se relevant and helpful" and because due process requires that "Fourth Amendment suppression questions . . . must be resolved through disclosure and adversarial litigation." No decision that Muhtorov cites holds that information of any kind is *always* relevant and helpful regardless of the circumstances. Whether information is relevant and helpful necessarily depends on the circumstances involved, including, among other things, the nature of the charges, the anticipated defenses, and the nature of the information at issue. As this Court's review of the classified record will confirm, any classified information that the district court permitted the government to withhold from discovery pursuant to CIPA Section 4 rulings was not relevant and helpful to Muhtorov's suppression claims, and any substitutions the district court approved gave Muhtorov substantially the same ability to make

his suppression arguments as would disclosure of the specific classified information at issue.

Moreover, Muhtorov cites no decision holding that it is a violation of due process to withhold classified information from discovery where, as here, the information is not relevant and helpful to the defense. *See*, *e.g.*, *Pringle*, 751 F.2d at 427-28 (rejecting due process challenge to order withholding classified information that was not relevant and helpful). And, as discussed above, none of the cases that Muhtorov cites holds or even suggests that the Due Process Clause requires the disclosure to a defendant of all investigative tools that it has used.

IV. The Delay In Bringing Muhtorov To Trial Was The Result Of the Complexity of the Case And His Own Litigation Strategy

Muhtorov claims (Br. 88-96) that the delay of more than six years between his arrest and trial violated the Sixth Amendment. Muhtorov joins in Jumaev's similar speedy trial claim. *See id.* at 89 (citing Fed. R. App. P. 28(i)). The government has responded to Jumaev's claim in its brief in No. 18-1296 and refers the Court to that response, most of which applies equally to Muhtorov. The discussion below focuses principally on Muhtorov's separate contentions. Because Muhtorov only belatedly demanded a speedy trial and is himself substantially responsible for the delay, and because he cannot demonstrate significant prejudice, his speedy trial claim fails.

A. The Issue Below and Standard of Review

Muhtorov first moved to dismiss on speedy trial grounds on March 29, 2017. ROA Vol. 15 at 282 (#1327). Following argument, the district court concluded that "the actions that have been taken so far are reasonable" and denied the motion. ROA Vol. 12 at 554 (#1425). Muhtorov filed a second motion to dismiss on May 22, 2018, during jury selection. ROA Vol. 15 at 522 (#1839). The court denied that motion, following argument, on May 24, 2018. ROA Vol. 20 at 146-50 (#1933). This Court reviews constitutional questions *de novo* but accepts the district court's factual findings unless clearly erroneous. *United States v. Hicks*, 779 F.3d 1163, 1167 (10th Cir. 2015).

B. Argument

In evaluating a Sixth Amendment speedy trial claim, this Court considers four factors identified in *Barker v. Wingo*, 407 U.S. 514, 530-33 (1972): (1) length of delay, (2) the reason for the delay, (3) the defendant's assertion of his right, and (4) prejudice to the defendant. None of the factors is determinative, and they must be considered together with all relevant circumstances. *Id.* at 533.

1. Length of the Delay

Muhtorov and Jumaev are similarly situated as to this factor. In *Doggett v. United States*, 505 U.S. 647 (1992), the Supreme Court noted that "[d]epending on the nature of the charges, the lower courts have generally found postaccusation

delay 'presumptively prejudicial' at least as it approaches one year." *Id*. at 652 n.1 (citations omitted); s*ee also Hicks,* 779 F.3d at 1167-68. However, this presumption does not establish a "statistical probability of prejudice; it simply marks the point at which courts deem the delay unreasonable enough to trigger the *Barker* enquiry." *Doggett*, 505 U.S. at 652 n.1. Without conceding actual prejudice, the government agrees that the delay here warrants consideration of the remaining *Barker* factors.

2. Reasons for the Delay

The delay between Muhtorov's arrest and trial resulted principally from (1) the complexity of the case—including voluminous discovery involving classified information and requiring translation from Uzbek and Tajik—and (2) Muhtorov's own aggressive litigation strategy. *See United States v. Muhtorov*, 702 F. App'x 694, 696 (10th Cir. 2017) (unpublished) (listing the "confluence of factors" contributing to delay). As discussed in the government's brief in *Jumaev*, the investigation of Muhtorov and Jumaev resulted in the government's acquisition of huge volumes of evidence, including information obtained through FISA, that had to be reviewed for possible disclosure to the defense in discovery. Much of that evidence involved classified information that the government had to submit to the district court for review and consideration under the procedures set forth in CIPA to ensure that national security was protected in a manner consistent with the

defendants' right to receive and present evidence in his defense. Moreover, many of the communications that were acquired by the government and subject to possible discovery were in Uzbek or Tajik, and security-cleared translators for those languages were scarce. The translation and review of those communications was unavoidably time-consuming. Moreover, this case involved the use or disclosure of evidence obtained or derived from Section 702, and the defendants' motions to suppress that evidence raised what were then novel and substantial statutory and constitutional questions. Those questions required extensive briefing and careful consideration by the district court.

Muhtorov's aggressive litigation strategy also substantially contributed to the delay. His unsuccessful efforts to suppress evidence obtained or derived through traditional FISA and Section 702 and to gain access to classified information, including disclosures about the government's investigative techniques, were time-consuming for the parties and the district court. As discussed at greater length in our brief in *Jumaev*, both defendants also aggressively litigated many other aspects of the case. Even a cursory review of the record reveals that Muhtorov's priority was not moving his case swiftly to trial, but vigorously litigating a host of pretrial matters.

For most of the case, Muhtorov and Jumaev were joined for trial. Even after the court granted Muhtorov's severance motion in November 2016, the co-

defendants continued their joint motions practice. Hence, most of the reasons for the delay in Jumaev's case apply also to Muhtorov. In denying Muhtorov's second motion to dismiss, the district court did not fault the government, but attributed the delay to voluminous evidence, issues of first impression, translation difficulties, and pretrial litigation. The court observed that it had issued "over 1,000 orders during this period of time," correctly finding that "the case has always been one of great difficulty from the beginning, because it involves on the one hand, national security that has to be counterbalanced by the obligation to present a fair trial." *See* ROA Vol. 20 at 148-49.

Muhtorov separately claims that "the Section 702 suppression litigation delayed the trial" and "could have been completed far earlier" but for what he describes as the government's "belated" notice of its intent to use evidence obtained or derived from Section 702 collection as to which he was aggrieved. Br. 90. Contrary to Muhtorov's claim, however, the government's Section 702 notice was timely. FISA requires the government to file its notice "prior to trial," which it did here. *See* 50 U.S.C. §§ 1806(c), 1881e(a). Indeed, the government filed its Section 702 notice on October 25, 2013, roughly 20 months after the first indictment and initial FISA notice, and well before either party was close to ready for trial. *See* ROA Vol. 1 at 552. To be sure, the ensuing litigation on the defendants' motions to suppress the Section 702-derived evidence and to disclose

classified materials relating to the Section 702 acquisitions took significant time in light of the novel and substantial questions involved. And, as the district court observed, the ACLU's appearance and participation in litigating those motions was also a delaying factor. ROA Vol. 7 at 14. Nevertheless, even after the district court's denial of the defendants' motions in November 2015, *see* ROA Vol. 3 at 115, the case still was not close to ready for trial, as discovery was incomplete and the defendants had other pending motions. *See*, *e.g.*, ROA Vol. 1 at 857 (#584), 878 (#590), 1082 (#652), 1157 (#658). Accordingly, Muhtorov is incorrect in asserting that the timing of the government's Section 702 notice was a prominent factor in delaying his trial.

Muhtorov is also wrong in claiming that even after his motion to sever was granted, "delays unique to . . . Jumaev's case continued to impact [him]." Br. 91. The district court granted Muhtorov's severance motion—made nearly five years after he was first charged—on two grounds: (1) at a joint trial, Jumaev might not testify and incriminating statements introduced against Jumaev might implicate Muhtorov, in violation of *Bruton v. United States*, 391 U.S. 123, 126 (1968); and (2) Muhtorov wished to call Jumaev as a witness at his trial to provide exculpatory testimony. ROA Vol. 15 at 234. In fact, Jumaev did testify at his own trial; and Muhtorov, who was tried second at his request, did not call Jumaev as a witness. Muhtorov tacitly concedes, as he must, that his severance motion delayed his trial.

The fact that the concerns underlying the severance motion never came to fruition does not make the resulting delay the government's fault.

3. Whether Muhtorov Asserted His Right to a Speedy Trial

Muhtorov waited over five years before filing his first motion claiming a speedy trial violation. *See* ROA Vol. 15 at 282. His second motion was not filed until over six years had passed. *See id.* at 522.[24] Although Muhtorov now claims that he "continuously asserted his right" to a speedy trial (Br. 92), the record shows otherwise. In denying Muhtorov's release pending trial, this Court noted that Muhtorov had, as of 2015, "acknowledged the lack of any speedy trial issues and conceded the pretrial process had taken a long time due to the case's complexity." *Muhtorov*, 702 F. App'x at 697. The government addresses this issue in its *Jumaev* brief, and most arguments raised there apply equally to Muhtorov.

4. Prejudice

Muhtorov claims that because of the length of the delay he need not show prejudice. Br. 92. As the government shows in *Jumaev*, however, that is incorrect: this Court considers only the delay attributable to the government's negligence in deciding whether to require a specific showing of prejudice. *Hicks*, 779 F.3d at 1168-69. Here, as the district court found, the delay largely resulted from the

[24] Muhtorov also filed several *pro se* motions—which were stricken—but these also were not filed until more than five years had passed since his arrest and indictment. *See* ROA Vol. 1 at 113-14.

novelty and complexity of the case, not from any fault of the government. And, as discussed above, Muhtorov's litigation strategy also substantially contributed to the delay.

Muhtorov claims prejudice on three grounds: (a) oppressive pretrial incarceration; (b) anxiety and concern; and (c) impairment of his defense. The last is the "most important." *Hicks*, 779 F.3d at 1169.

(a) Oppressive pretrial incarceration

Muhtorov claims that his pretrial detention was "neither typical[] nor easy" (Br. 93), but he has failed to show that it was oppressive. With respect to the length of the detention, this Court held in 2017 that Muhtorov must remain in custody notwithstanding "[t]he delay in proceeding to trial." *Muhtorov*, 702 F. App'x at 696, 701-02. Regarding the conditions of his pretrial confinement, Muhtorov cites a 2012 transcript that is not in the record on appeal for the proposition that he complained following his arrest about inadequate access to a telephone and to religious and other reading materials. *See* Br. 93 (citing Doc. 56 at 10). But it appears from a second cited transcript that the district court addressed that complaint relatively promptly by causing Muhtorov to be transferred to another facility. *See id*. (citing ROA Vol. 12 at 567-69). As Muhtorov claims, he spent time at numerous facilities. *Id.* (citing ROA Vol. 18 at 441). The presentence report that he cites, however, shows that his religious

preferences were respected and that he had no serious problems while detained. *See* ROA Vol. 18 at 441. Muhtorov also complains that his incarceration resulted in long periods without physical interactions with his family. Br. 93. But restrictions on contact visits are not uncommon. *See*, *e.g.*, *Block v. Rutherford*, 468 U.S. 576, 576–77 (1984) (explaining that "[t]here are many justifications for denying contact visits entirely, rather than attempting the difficult task of establishing a program of limited visits," and holding that such visits are not constitutionally required).

(b) Anxiety and Concern

As Muhtorov concedes (Br. 94), he must show "some special harm which distinguishes" his case from that of any other arrestee awaiting trial. *United States v. Frias*, 893 F.3d 1268, 1273 (10th Cir.), *cert. denied*, 139 S. Ct. 466 (2018) (citing *Hicks*, 779 F.3d at 1169) (further citation omitted). He cites the observation of a social worker, contained in the presentence report, that Muhtorov looked at one point like he was not "coping well." Br. 94. However, the presentence report also states, under the heading "Mental and Emotional Health," that "[t]he defendant reported he has never participated in mental health treatment, and he does not believe he is in need of such. He indicated his weekly family visits, working out, and reading, have helped him cope with his lengthy period of

incarceration." ROA Vol. 18 at 457. Muhtorov has not shown that he suffered any "special harm."

(c) Impairment of the defense

Muhtorov insists (Br. 95) that his defense was impaired when a witness, Vasila Inoyatova, died before trial. He asserts that Inoyatova would have testified regarding his human rights work in Uzbekistan. This was the basis of his second motion to dismiss. ROA Vol. 15 at 522. To show this form of prejudice, a defendant must demonstrate with specificity how the evidence would have aided his defense; how government delay caused the evidence to be actually lost; and whether he took appropriate steps to preserve the evidence. *See United States v. Medina*, 918 F.3d 774, 783 (10th Cir.), *cert. denied*, 139 S. Ct. 2706 (2019).

Muhtorov has not shown that the delay caused evidence to be lost. Although Inoyatova died shortly before trial, abundant evidence existed, and, as discussed below, was presented at trial, regarding Muhtorov's previous human rights work. And Muhtorov could have recorded and preserved Ms. Inoyatova's testimony, but did not. Ms. Inoyatova was 62 years old, lived and worked thousands of miles away, in a dangerous part of the world—particularly for human rights workers. Surely, Muhtorov's counsel might have anticipated that Ms. Inoyatova, for any number of reasons, might become unavailable as a witness.

But the primary problems with Muhtorov's argument are that Inoyatova's proffered testimony did not counter the criminal charges against him and, if presented, would have been cumulative. The government does not contest that Inoyatova could have testified regarding Muhtorov's human rights work in Uzbekistan and the oppressive regime under which people suffered. But Muhtorov was charged with providing material support to a foreign terrorist organization, while in the United States, during 2011 and 2012. His involvement in human rights work in Uzbekistan in prior years is not a defense to the charges. As the district court observed, Inoyatova's proffered testimony "does not go to the gravamen of the charge. It goes to an explanation of motivation and of background and not to the essence of the charge." ROA Vol. 20 at 149.

Moreover, it was undisputed that Muhtorov had been involved in human rights work in Uzbekistan. Numerous defense witnesses testified to this. *See, e.g.*, ROA Vol. 20 at 1358 (defendant's brother); *id*. at 1399-1401, 1407, 1412-13 (Human Rights Watch witness); *id*. at 1306, 1311, 1314, 1319-20 (journalist and human rights worker). And Muhtorov himself testified regarding his human rights work. *Id*. at 1052, 1078-80, 1083, 1243. Finally, in closing argument, the prosecutor acknowledged Muhtorov's prior human rights work in Uzbekistan, but argued based on abundant trial evidence that "[Muhtorov] rejected his prior human

rights worker self, and he chose an entirely new path, radical Islamic jihadism." ROA Vol. 20 at 1552-53.

CONCLUSION

For the foregoing reasons, the judgment should be affirmed.

ORAL ARGUMENT STATEMENT

In light of the volume of the record and significance of the issues, oral argument may be helpful to the Court.

Respectfully submitted,

JASON R. DUNN
United States Attorney

JAMES C. MURPHY
Assistant U.S. Attorney
District of Colorado

JOHN C. DEMERS
Assistant Attorney General

s/ Joseph Palmer
JOSEPH PALMER
STEVEN L. LANE
Attorneys
National Security Division
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530
202-353-9402
Joseph.Palmer@usdoj.gov

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation set forth in this Court's February 5, 2020, Order granting leave to file an oversized brief not to exceed 18,250 words. This brief contains 18,137 words, according to the Microsoft Word software used, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

/s/ Joseph Palmer
JOSPEPH PALMER
Attorney for the United States

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

(1) all required privacy redactions have been made;

(2) if required to file additional hard copies, that the ECF submission is an exact copy of those documents;

(3) the digital submission has been scanned for viruses with the most recent version of Windows Defender, Version 1.209.699.0, dated 2/10/20, and according to the program is free of viruses.

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.

/s/ Joseph Palmer
JOSPEPH PALMER
Attorney for the United States

CERTIFICATE OF SERVICE

I hereby certify that on this 10th day of February, 2020, I electronically filed the foregoing **BRIEF FOR THE UNITED STATES** with the Clerk of the Court for the United States Court of Appeals for the Tenth Circuit, using the CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

/s/ Joseph Palmer
JOSPEPH PALMER
Attorney for the United States