

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA)	
)	
Plaintiff)	No. 16 CR 181
v.)	
)	Judge Sara L. Ellis
)	
AWS MOHAMMED YOUNIS AL-JAYAB)	
)	
Defendant)	

**GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN SUPPORT OF ITS
MOTION FOR AN *EX PARTE*, *IN CAMERA* REVIEW TO DETERMINE THE
LEGALITY OF COLLECTION PURSUANT TO THE FOREIGN
INTELLIGENCE SURVEILLANCE ACT ("FISA") AND IN OPPOSITION TO
DEFENDANT'S MOTIONS FOR NOTICE OF SURVEILLANCE TECHNIQUES,
FOR DISCOVERY, AND TO SUPPRESS EVIDENCE OBTAINED OR DERIVED
FROM SECTION 702 OF FISA**

JOEL R. LEVIN
Acting United States Attorney
Northern District of Illinois

DANA J. BOENTE
Acting Assistant Attorney General for
National Security

Barry Jonas
Shoba Pillay
Assistant U.S. Attorneys
Northern District of Illinois

Andrew Sigler
Trial Attorney
Counterterrorism Section
National Security Division
Department of Justice

Steven L. Lane
Attorney Advisor
Office of Law and Policy
National Security Division
Department of Justice

Jeremy S. Balint and Chad Davis
Attorney Advisors
Office of Intelligence
National Security Division
Department of Justice

TABLE OF CONTENTS

I. <u>INTRODUCTION</u>	1
A. <u>OVERVIEW</u>	2
B. <u>SUMMARY OF THE ARGUMENT</u>	5
1. Section 702 Is Constitutional	5
2. The Collection in This Case Was Lawfully Authorized and Conducted	6
3. The Defendant's Motions for Additional Notice and Discovery Should Be Denied	6
II. <u>BACKGROUND</u>	7
A. <u>FACTUAL BACKGROUND</u>	7
1. Defendant Aws Mohammed Younis Al-Jayab	7
2. The Defendant's Plans to Travel to Syria	7
3. The Defendant's Travel to Turkey and Syria	14
4. The Defendant's Return to Turkey and the United States	18
5. [CLASSIFIED MATERIAL REDACTED]	18
6. USCIS and FBI Interviews	18
B. <u>CHARGES AND PROCEDURAL HISTORY</u>	19
C. <u>OVERVIEW OF THE SECTION 702 COLLECTION AT ISSUE</u>	20
III. <u>OVERVIEW OF FISA AND THE FISA AMENDMENTS ACT</u>	20
A. <u>THE FOREIGN INTELLIGENCE SURVEILLANCE ACT</u>	20
B. <u>THE PROTECT AMERICA ACT</u>	23
C. <u>THE FISA AMENDMENTS ACT OF 2008</u>	25
1. The Government's Submission to the FISC	28
2. The FISC's Order(s) and Opinion(s)	29
3. Implementing Section 702 Authority	30
4. Targeting and Minimization Procedures	32
a. Targeting Procedures	33
b. Minimization Procedures	36
5. Oversight	38
6. District Court Review of FISC Orders and Section 702 Collection	40
IV. <u>THE DEFENDANT'S CONSTITUTIONAL ARGUMENTS LACK MERIT</u>	43
A. <u>THE ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION UNDER SECTION 702 IS LAWFUL UNDER THE FOURTH AMENDMENT</u>	43
1. There Is No Judicial Warrant Requirement Applicable to Foreign Intelligence Collection Targeted at Foreign Persons Abroad	46
a. The Fourth Amendment Generally Does Not Apply to Non-U.S. Persons Abroad	46

b. The Incidental Collection of Communications of Persons Protected by the Fourth Amendment Pursuant to Intelligence Collection Lawfully Targeting Non-U.S. Persons Located Outside the United States Does Not Trigger a Warrant Requirement.....	48
c. The Location of the Search Does Not Trigger a Warrant Requirement	55
2. The Foreign Intelligence Exception Applies	56
a. The “Special Needs” Doctrine	56
b. The Foreign Intelligence Exception	58
c. The Government’s Purpose in Section 702 Collection Goes Beyond Ordinary Crime Control.....	61
d. A Warrant or Probable Cause Requirement Would Be Impracticable	63
e. A Warrant Requirement Would Inappropriately Interfere with Executive Branch Discretion in the Collection of Foreign Intelligence.....	65
f. Section 702 Falls Within the Scope of the Foreign Intelligence Exception	66
3. Foreign Intelligence Collection Pursuant to Section 702 Is Reasonable.....	68
a. Acquisitions Under Section 702 Advance the Government’s Compelling Interest in Obtaining Foreign Intelligence Information to Protect National Security	73
b. U.S. Persons and Persons in the United States Have, at Most, Limited Expectations of Privacy in Electronic Communications With Non-U.S. Persons Outside the United States.....	76
c. Stringent Safeguards and Procedures Protect the Privacy Interests of U.S. Persons and Others Whose Communications are Acquired.....	78
i. Senior officials certify that the government’s procedures satisfy statutory requirements.....	79
ii. Prior Judicial review	80
iii. Targeting procedures ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States	81
iv. A significant purpose of the acquisition must be to obtain foreign intelligence information	83
v. Minimization procedures protect the privacy of U.S. persons whose communications are acquired.....	84
vi. Executive Branch, Congressional, and Judicial oversight	92
d. Collection Under Section 702 Has Sufficient Particularity.....	94
B. <u>SECTION 702 IS CONSISTENT WITH ARTICLE III</u>	97

C. <u>THE GOOD FAITH EXCEPTION APPLIES</u>	102
V. <u>THE SECTION 702 INFORMATION WAS LAWFULLY ACQUIRED AND ACQUISITIONS WERE CONDUCTED IN CONFORMITY WITH ORDER(S) OF AUTHORIZATION OR APPROVAL</u>	105
A. <u>[CLASSIFIED MATERIAL REDACTED]</u>	105
B. <u>THE APPLICABLE TARGETING PROCEDURES MET THE STATUTORY REQUIREMENTS</u>	105
C. <u>THE APPLICABLE MINIMIZATION PROCEDURES MET THE STATUTORY REQUIREMENTS</u>	105
D. <u>[CLASSIFIED MATERIAL REDACTED]</u>	105
1. Relevant Facts	105
a. <u>[CLASSIFIED MATERIAL REDACTED]</u>	105
b. <u>[CLASSIFIED MATERIAL REDACTED]</u>	105
2. <u>[CLASSIFIED MATERIAL REDACTED]</u>	105
a. <u>[CLASSIFIED MATERIAL REDACTED]</u>	105
b. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
c. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
d. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
3. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
a. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
b. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
4. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
a. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
b. <u>[CLASSIFIED MATERIAL REDACTED]</u>	106
VI. <u>THE TITLE III FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE PHYSICAL SEARCH WAS MADE IN CONFORMITY WITH ORDER(S) OF AUTHORIZATION OR APPROVAL</u>	106
A. <u>STANDARD OF REVIEW</u>	107
1. Probable Cause Standard	108
2. Standard of Review of Certifications	108
B. <u>OVERVIEW OF THE FISA AUTHORITIES</u>	110
1. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
2. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
C. <u>THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD</u>	110
1. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
2. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
3. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
a. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
b. <u>[CLASSIFIED MATERIAL REDACTED]</u>	110
4. Conclusion: There Was Sufficient Probable Cause to Establish that the Information Acquired from the Targeted Facilities, Places, Property, or Premises Was Lawfully Acquired	111

D. <u>THE CERTIFICATIONS IN THE APPLICATION(S) COMPLIED WITH FISA</u>	111
1. Foreign Intelligence Information.....	111
2. "A Significant Purpose"	111
3. Information Not Reasonably Obtainable Through Normal Investigative Techniques.....	111
E. <u>PHYSICAL SEARCH WAS CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OF APPROVAL</u>	111
1. The Standard Minimization Procedures	111
2. The FISA Information Was Appropriately Minimized	112
VII. <u>THE DEFENDANT'S MOTIONS FOR ADDITIONAL NOTICE AND DISCOVERY SHOULD BE DENIED</u>	113
VIII. <u>CONCLUSION</u>	119

TABLE OF AUTHORITIES

Cases

<i>[Caption Redacted]</i> , 2011 WL 10945618 (FISA Ct. Oct. 3, 2011)	<i>passim</i>
<i>[Caption Redacted]</i> , 2011 WL 10947772 (FISA Ct. Nov. 30, 2011)	31, 86, 94
<i>[Caption Redacted]</i> (FISA Ct. Aug. 26, 2014)	80, 95
<i>[Caption Redacted]</i> (FISA Ct. Nov. 6, 2015) (“ <i>Nov. 2015 FISC Op.</i> ”)	72, 80, 92
<i>[Caption Redacted]</i> (FISA Ct. Apr. 26, 2017) (“ <i>April 2017 FISC Op.</i> ”)	31, 33
<i>Acosta v. Gonzales</i> , 439 F.3d 550 (9th Cir. 2006)	118
<i>Amnesty Int’l. USA v. Clapper</i> , 667 F.3d 163 (2d Cir. 2011)	78
<i>Bloate v. United States</i> , 559 U.S. 196 (2010)	117
<i>Boroian v. Mueller</i> , 616 F.3d 60 (1st Cir. 2010)	87
<i>Branzburg v. Hayes</i> , 408 U.S. 665 (1972)	91
<i>Bhd. of Maintenance of Way Emp. v. CSX Transp., Inc.</i> , 478 F.3d 814 (7th Cir. 2007)	118
<i>Camara v. Municipal Ct.</i> , 387 U.S. 523 (1967)	102
<i>Cannon v. University of Chicago</i> , 441 U.S. 677 (1979)	67
<i>Cassidy v. Chertoff</i> , 471 F.3d 67 (2d Cir. 2006)	61
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000)	57, 67
<i>City of Los Angeles v. Patel</i> , 135 S. Ct. 2443 (2015)	47
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013)	<i>passim</i>
<i>Couch v. United States</i> , 409 U.S. 322 (1973)	76
<i>Davis v. United States</i> , 564 U.S. 229 (2011)	103, 104
<i>Dean v. United States</i> , 556 U.S. 568 (2009)	116
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001)	57
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978)	108
<i>Gozlon-Peretz v. United States</i> , 498 U.S. 395 (1991)	117, 118
<i>Griffin v. Wisconsin</i> , 483 U.S. 868 (1987)	57, 58
<i>Guest v. Leis</i> , 255 F.3d 325 (6th Cir. 2001)	77
<i>Haig v. Agee</i> , 453 U.S. 280 (1981)	73
<i>Halperin v. Kissinger</i> , 606 F.2d 1192 (D.C. Cir. 1979)	101
<i>Herring v. United States</i> , 555 U.S. 135 (2009)	104
<i>Hoffa v. United States</i> , 385 U.S. 293 (1966)	76
<i>Holder v. Humanitarian Law Project</i> , 561 U.S. 1 (2010)	73
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983)	107
<i>Illinois v. Krull</i> , 480 U.S. 340 (1987)	102, 103, 104
<i>Illinois v. McArthur</i> , 531 U.S. 326 (2001)	69
<i>In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)</i> , 830 F. Supp. 2d 114 (E.D. Va. 2011)	98
<i>In re Certified Question of Law</i> , --- F.3d. ---, No. FISCER 16-01, 2016 WL 8923919, (FISA Ct. Rev. Apr. 14, 2016)	73
<i>In re DNI/AG Certification</i> , No. 702(i)-08-01 (FISA Ct. Rev. Sept. 4, 2008) (“ <i>Sept. 2008 FISC Op.</i> ”)	<i>passim</i>

<i>In re Directives Pursuant to Section 105B of FISA</i> , 551 F.3d 1004 (FISA Ct. Rev. 2008).....	<i>passim</i>
<i>In re Grand Jury Investigation</i> , 431 F. Supp. 2d 584 (E.D. Va. 2006)	118
<i>In re Grand Jury Proceedings of Special Apr. 2002 Grand Jury</i> , 347 F.3d 197 (7th Cir. 2003)	42, 109
<i>In re Grand Jury Subpoena (Kitzhaber)</i> , 828 F.3d 1083 (9th Cir. 2016).....	78
<i>In re Kevork</i> , 634 F. Supp. 1002 (C.D. Cal. 1985).....	98
<i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002)	<i>passim</i>
<i>In re Terrorist Bombings of U.S. Embassies</i> , 552 F.3d 157 (2d Cir. 2008)....	53, 65, 73, 74
<i>Jabara v. Webster</i> , 691 F.2d 272 (6th Cir. 1982)	87, 88
<i>Johnson v. Quander</i> , 440 F.3d 489 (D.C. Cir. 2006).....	87
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	56
<i>MacWade v. Kelly</i> , 460 F.3d 260 (2d Cir. 2006).....	59, 60
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	89
<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013)	<i>passim</i>
<i>Minnesota v. Carter</i> , 525 U.S. 83 (1998)	76
<i>Mistretta v. United States</i> , 488 U.S. 361 (1989)	97, 98, 99
<i>Morrison v. Olson</i> , 487 U.S. 654 (1988)	97, 98
<i>Nat'l Treasury Emps. Union v. Von Raab</i> , 489 U.S. 656 (1989)	43, 69
<i>New Jersey v. T.L.O.</i> , 469 U.S. 325 (1985).....	43, 58
<i>Pennsylvania v. Mimms</i> , 434 U.S. 106 (1977)	43, 44
<i>Pennsylvania v. Ritchie</i> , 480 U.S. 59 (1987)	113, 114
<i>Samson v. California</i> , 547 U.S. 843 (2006).....	57, 69, 70
<i>Scott v. United States</i> , 436 U.S. 128 (1978)	112
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968).....	44
<i>United States v. Abu-Jihaad</i> , 630 F.3d 102 (2d Cir. 2010)	<i>passim</i>
<i>United States v. Agurs</i> , 427 U.S. 97 (1976).....	113
<i>United States v. Ahmed</i> , No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007 (N.D. Ga. Mar. 19, 2009).....	107, 108, 109
<i>United States v. Omar Al Hardan</i> , 16 CR 03 (S.D. Tex.).....	10
<i>United States v. Aws Mohammed Younis Al-Jayab</i> , 16 CR 08 (E.D. Cal.).....	<i>passim</i>
<i>United States v. Alwan</i> , No. 1:11-CR-13-R, 2012 WL 399154 (W.D. Ky. Feb. 7, 2012)	109
<i>United States v. Apple</i> , 915 F.2d 899 (4th Cir. 1990).....	118
<i>United States v. Aref</i> , 285 F. App'x 784 (2d Cir. 2008).....	118
<i>United States v. Badia</i> , 827 F.2d 1458 (11th Cir. 1987)	108, 109
<i>United States v. Bagley</i> , 473 U.S. 667 (1985)	114
<i>United States v. Barona</i> , 56 F.3d 1087 (9th Cir. 1995)	53
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982).....	93, 116
<i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000).....	<i>passim</i>
<i>United States v. Brewer</i> , 204 F. App'x 205 (4th Cir. 2006)	104
<i>United States v. Brown</i> , 484 F.2d 418 (5th Cir. 1973)	58, 59, 61
<i>United States v. Buck</i> , 548 F.2d 871 (9th Cir. 1977)	58
<i>United States v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974)	49, 58, 61

<i>United States v. Campa</i> , 529 F.3d 980 (11th Cir. 2008)	108, 109
<i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987)	108
<i>United States v. Colon</i> , No. 97-CR-659, 1998 WL 214714 (N.D. Ill. Apr. 21, 1998).....	113
<i>United States v. Daoud</i> , No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014).....	42
<i>United States v. Daoud</i> , 755 F.3d 479 (7th Cir. 2014), <i>supplemented</i> , 761 F.3d 678 (7th Cir. 2014), <i>cert. denied</i> , 135 S. Ct. 1456 (2015).....	3, 42
<i>United States v. Duggan</i> , 743 F.2d 59 (2d Cir. 1984).....	108, 109
<i>United States v. Duka</i> , 671 F.3d 329 (3d Cir. 2011).....	<i>passim</i>
<i>United States v. El-Mezain</i> , 664 F.3d 467 (5th Cir. 2011)	42, 43, 108
<i>United States v. Figueroa</i> , 757 F.2d 466 (2d Cir. 1985)	49
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008)	78
<i>United States v. Garcia</i> , 413 F.3d 201 (2d Cir. 2005).....	110
<i>United States v. Glover</i> , 736 F.3d 509 (D.C. Cir. 2013).....	104
<i>United States v. Goffer</i> , 721 F.3d 113 (2d Cir. 2013).....	91
<i>United States v. Griebel</i> , 312 F. App'x 93 (10th Cir. 2008)	113
<i>United States v. Hammoud</i> , 381 F.3d 316 (4th Cir. 2004).....	107, 112
<i>United States v. Hasbajrami</i> , No. 11-CR-623 (JG), 2016 WL 1029500 (E.D.N.Y Mar. 8, 2016)	<i>passim</i>
<i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007)	77
<i>United States v. Isa</i> , 923 F.2d 1300 (8th Cir. 1991)	42
<i>United States v. Ishak</i> , 277 F.R.D. 156 (E.D. Va. 2011).....	114
<i>United States v. Islamic Am. Relief Agency (IARA)</i> , No. 07-00087-CR-W-NKL, 2009 WL 5169536 (W.D. Mo. Dec. 21, 2009).....	109, 110, 112
<i>United States v. Kahn</i> , 415 U.S. 143 (1974)	49
<i>United States v. Kashmiri</i> , No. 09-CR-830-4, 2010 WL 4705159 (N.D. Ill. Nov. 10, 2010)	107, 109
<i>United States v. King</i> , 55 F.3d 1193 (6th Cir. 1995)	77
<i>United States v. Knights</i> , 534 U.S. 112 (2001)	56, 76
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	102, 103
<i>United States v. Lifshitz</i> , 369 F.3d 173 (2d Cir. 2004)	77
<i>United States v. Londono-Cardoña</i> , No. 05-10304-GAO, 2008 WL 313473 (D. Mass. Feb. 1, 2008).....	118
<i>United States v. Malekzadeh</i> , 855 F.2d 1492 (11th Cir. 1988).....	104
<i>United States v. Martinez-Fuerte</i> , 428 U.S. 543 (1976).....	58
<i>United States v. Marzook</i> , 435 F. Supp. 2d 778 (N.D. Ill. 2006)	103
<i>United States v. McKinnon</i> , 721 F.2d 19 (1st Cir. 1983).....	52
<i>United States v. Megahey</i> , 553 F. Supp. 1180 (E.D.N.Y 1982)	100
<i>United States v. Miller</i> , 425 U.S. 435 (1976)	76
<i>United States v. Mohamud</i> , No. 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or. June 24, 2014), <i>aff'd</i> , 843 F.2d 420 (9th Cir. 2016)	<i>passim</i>
<i>United States v. Mohamud</i> , 843 F.3d 420 (9th Cir. 2016)	<i>passim</i>
<i>United States v. Moore</i> , 41 F.3d 370 (8th Cir. 1994)	104
<i>United States v. Mubayyid</i> , 521 F. Supp. 2d 125 (D. Mass. 2007).....	103, 104, 112

<i>United States v. Muhtorov</i> , No. 12-cr-00033-JLK (slip op.) (D. Colo. Nov. 19, 2015).....	46, 73, 89
<i>United States v. Nicholson</i> , No. 09-CR-40-BR, 2010 WL 1641167 (D. Or. Apr. 21, 2010).....	107, 108
<i>United States v. Ning Wen</i> , 477 F.3d 896 (7th Cir. 2007).....	102
<i>United States v. Omar</i> , 786 F.3d 1104 (8th Cir. 2015).....	42
<i>United States v. Phillips</i> , 854 F.2d 273 (7th Cir. 1988).....	113
<i>United States v. Rahman</i> , 861 F. Supp. 247 (S.D.N.Y. 1994).....	109
<i>United States v. Rice</i> , 478 F.3d 704 (6th Cir. 2007).....	104
<i>United States v. Rosen</i> , 447 F. Supp. 2d 538 (E.D. Va. 2006).....	107, 108
<i>United States v. Salerno</i> , 481 U.S. 739 (1987).....	47
<i>United States v. Solomonyan</i> , 451 F. Supp. 2d 626 (S.D.N.Y. 2006).....	104
<i>United States v. Sherifi</i> , 793 F. Supp. 2d 751 (E.D.N.C. 2011).....	108
<i>United States v. Stokes</i> , 726 F.3d 880 (7th Cir. 2013).....	53
<i>United States v. Tortorello</i> , 480 F.2d 764 (2d Cir. 1973).....	101
<i>United States v. Truong Dinh Hung</i> , 629 F.2d 908 (4th Cir. 1980).....	passim
<i>United States v. U.S. District Court (Keith)</i> , 407 U.S. 297 (1972).....	60, 108
<i>United States v. U.S. Gypsum Co.</i> , 333 U.S. 364 (1948).....	109, 110
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990).....	passim
<i>United States v. Warsame</i> , 547 F. Supp. 2d 982 (D. Minn. 2008).....	107, 108, 109
<i>United States v. Warshak</i> , 631 F. 3d 266 (6th Cir. 2010).....	62, 77, 78
<i>United States v. White</i> , 401 U.S. 745 (1971).....	49, 76
<i>United States v. Yonn</i> , 702 F.2d 1341 (11th Cir. 1983).....	55, 56
<i>Vernonia Sch. Dist. 47J v. Acton</i> , 515 U.S. 646 (1995).....	56, 57
<i>Washington v. Glucksberg</i> , 521 U.S. 702 (1997).....	47, 48
<i>Youngstown Sheet & Tube Co. v. Sawyer</i> , 343 U.S. 579 (1952).....	60, 96
<i>Zweibon v. Mitchell</i> , 516 F.2d 594 (D.C. Cir. 1975).....	59

Statutes

18 U.S.C. § 2517.....	91
18 U.S.C. § 3504.....	117
50 U.S.C. § 1801.....	passim
50 U.S.C. § 1803.....	21
50 U.S.C. § 1804.....	21
50 U.S.C. § 1805.....	20, 21, 24
50 U.S.C. § 1806.....	passim
50 U.S.C. § 1821.....	passim
50 U.S.C. § 1825.....	passim
50 U.S.C. § 1881a.....	passim
50 U.S.C. § 1881b.....	25
50 U.S.C. § 1881c.....	25
50 U.S.C. § 1881e.....	passim
50 U.S.C. § 1881f.....	38, 92

Other Authorities

Exec. Order No. 12333.....	22
<i>Foreign Intelligence Surveillance Act: Hearings on S. 743, S. 1888, and S. 3197 Before the Subcomm. on Crim. Laws and Procedures of the S. Judiciary Comm., 94th Cong. (1976)</i>	22
H.R. Rep. No. 112-645 (2012)	74, 75, 93
<i>Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intel., 110th Cong. (2007)</i>	23, 24
Privacy and Civil Liberties Oversight Bd., <i>Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act</i> (July 2, 2014)	passim
Pub. L. No. 91-452, 84 Stat. 922 (1970)	118
Pub. L. No. 110-55, 121 Stat. 552 (2007)	passim
Pub. L. No. 110-261, 122 Stat. 2436 (2008)	passim
Pub. L. No. 112-238, 126 Stat. 1631 (2012)	25
S. Rep. No. 110-209 (2007)	24
S. Rep. No. 112-174 (2012)	74, 92, 93, 94
S. Rep. No. 95-701 (1978)	22, 112, 116
S. Rep. No. 95-604 (1977)	20
<i>The National Security Agency: Missions, Authorities, Oversight and Partnerships</i> (Aug. 9, 2013)	74
<i>Warrantless Surveillance and The Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II) Hearing Before the H. Judiciary Comm., 110th Cong. (2007)</i>	54

I. INTRODUCTION¹

The United States of America, by acting United States Attorney JOEL R. LEVIN, hereby files its unclassified memorandum in opposition to Defendant Aws Mohammed Younis al-Jayab's ("al-Jayab" or "defendant") Motion to Suppress Evidence Obtained or Derived from Warrantless Surveillance under Section 702 of the FISA Amendments Act² and supporting memorandum of law (Documents (Doc.) 47, 48), Motion for Notice of Surveillance Techniques Used During the Course of the Investigation (Doc. 52), and Motion for Discovery Regarding the Intelligence Agencies' Surveillance Pursuant to Executive Order 12333 (Doc. 51), each of which was filed on March 14, 2017.

Defendant seeks suppression of "all the fruits and derivatives of evidence obtained pursuant to Section 702 of the FISA-Amendments Act," arguing that Section 702 violates the Fourth Amendment with respect to warrantless surveillance, probable cause, particularity, and reasonableness, and further alleging that the Foreign Intelligence Surveillance Court (FISC) does not meet the neutrality requirement required for a tribunal reviewing a search warrant. (Docs. 47, 48) Defendant further seeks suppression by alleging that information collected under Section 702 may not have been lawfully acquired in this case. *Id.* In a separate motion, defendant also

¹ [CLASSIFIED MATERIAL REDACTED]

² The provision at issue here is properly referred to as Section 702 of FISA (Section 702). Section 702 of FISA, along with the rest of Title VII of FISA, was added by Section 101 of the FISA Amendments Act of 2008 ("FAA"). *See* FISA Amendments Act, Pub. L. 110-261 § 101, 122 Stat. 2436, 2437-59 (2008). The FISA Amendments Act itself has no Section 702. *See id.* § 1, 122 Stat. 2436 (table of contents).

seeks notice and disclosure of any information collected pursuant to Executive Order (E.O.) 12333. (Doc. 51) Finally, defendant seeks “notice and discovery of all the surveillance techniques that the government used” in this case, citing to the Fourth, Fifth, and Sixth Amendments to the Constitution, 18 U.S.C. § 3504, and Federal Rules of Criminal Procedure (F.R.C.P.) 12 and 16. (Doc. 52) As explained in detail herein, defendant’s arguments for suppression are all without merit, and the government has met its notice and disclosure obligations in this case. The government will address each argument in turn.

A. OVERVIEW

[CLASSIFIED MATERIAL REDACTED]

The defendant’s motion to suppress the Section 702-derived information³ has triggered this Court’s review pursuant to 50 U.S.C. §§ 1806(f) and 1881e(a),⁴ to determine whether the intelligence collection at issue herein was lawfully authorized and conducted in accordance with the requirements of Section 702.

As explained below, this Court should conduct an *in camera*, *ex parte* review of the Section 702 materials, in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1881e(a). Section 1806(f) provides that, where the Attorney General files an affidavit stating that “disclosure or an adversary hearing would harm the national security of the United States,” a district court “shall, notwithstanding any other law . . . review *in*

³ **[CLASSIFIED MATERIAL REDACTED]**

⁴ Section 1806(f) provides in pertinent part that the district court’s review of the legality of FISA collection is triggered “whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under [FISA].”

camera and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” 50 U.S.C. § 1806(f).⁵ This same procedure applies to motions to disclose Section 702-related materials or to suppress information obtained or derived from Section 702 acquisitions, which are deemed to be “electronic surveillance” conducted pursuant to Title I of FISA for purposes of such motions. 50 U.S.C. § 1881e(a). The Attorney General has filed such a declaration in this case.⁶ Once the Attorney General files a declaration, the court “may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance *only* where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” 50 U.S.C. § 1806(f) (emphasis supplied). If the court is able to assess the legality of the FISA collection by reviewing the government’s submissions *in camera* and *ex parte*, it must do so without disclosure to the defense. *United States v. Daoud*, 755 F.3d 479, 481-85, *supplemented*, 761 F.3d 678 (7th Cir. 2014), *cert. denied*, 135 S. Ct. 1456 (2015).

In opposition to the defendant’s motions, the government submits this classified memorandum of law for the Court’s *in camera*, *ex parte* review. A redacted version of

⁵ An “aggrieved person” is defined as the target of electronic surveillance or “any other person whose communications or activities were subject to electronic surveillance,” 50 U.S.C. § 1801(k), as well as “a person whose premises, property, information, or material is the target of physical search” or “whose premises, property, information, or material was subject to physical search.” 50 U.S.C. § 1821(2).

⁶ The Declaration and Claim of Privilege of the Attorney General of the United States is being filed as part of this *in camera*, *ex parte* submission, and is being provided to the defense. See Sealed Exhibit 1.

this memorandum, from which all classified information and all headers, footers, and paragraph classification markings have been redacted, is also being publicly filed and served on the defendant.⁷

[CLASSIFIED MATERIAL REDACTED]

The unclassified documents will be electronically filed in the public docket. All of the classified documents and the original Attorney General's Declaration and Claim of Privilege have been submitted to the Court, through the CISO, in a Sealed Appendix to this Memorandum for the Court's *in camera*, *ex parte* review.

The government expects that the Court will conclude from its *in camera*, *ex parte* review that: (1) Section 702 complies with the Fourth Amendment and Article III of the U.S. Constitution; (2) the acquisition, retention, and dissemination of foreign intelligence information pursuant to Section 702 were all lawfully authorized and conducted; (3) the fruits of the Section 702 collection at issue should not be suppressed; (4) disclosure to defendant of the Section 702 materials, the FISA materials, and the government's classified submission is unnecessary because the Court can make an accurate determination of the legality of the Section 702 and traditional FISA collection without disclosing such materials or portions thereof; (5) the physical search at issue in this case was both lawfully authorized and lawfully conducted in compliance with FISA; (6) the information obtained pursuant to traditional FISA and Section 702 should not be suppressed; (7) the government has fulfilled its notice and disclosure obligations; and (8) no hearing is required.

⁷ As a result of the redactions, the pagination and footnote numbering of the classified *in camera*, *ex parte* memorandum and the redacted unclassified memorandum may be different.

B. SUMMARY OF THE ARGUMENT

1. Section 702 Is Constitutional

The defendant argues in support of his motion to suppress that Section 702 violates the Fourth Amendment and Article III of the United States Constitution. As an initial matter, this Court's review should be limited to the constitutionality of the statute as applied to the acquisition of the information challenged in this case. As applied to the collection at issue here, Section 702 is constitutional. *See* Part IV.A., *infra*.

First, the Section 702 collection at issue was reasonable under the Fourth Amendment. The defendant was not targeted under Section 702. Instead, the collection lawfully targeted one or more non-U.S. persons located outside the United States, who generally are not protected by the Fourth Amendment, for foreign intelligence purposes. That the communications of U.S. persons or persons located inside the United States might be acquired incidentally during such collection does not trigger a warrant requirement. Nor does that fact render the collection unreasonable, in light of the compelling national security interests at stake and the extensive procedural safeguards that have been incorporated into the program to protect the privacy interests of U.S. persons. *See* Part IV.A.1.-3., *infra*.

Second, Section 702, in requiring the FISC to review the government's proposed certification(s) and implementing procedures, does not place the FISC in a role inconsistent with that accorded to Article III courts under the Constitution. The FISC's role under Section 702 is similar to that of other federal courts which review *ex*

parte applications for warrants and Title III wiretap orders. As such, Section 702 is entirely consistent with governing Article III principles. *See* Part IV.B., *infra*.

2. The Collection in this Case Was Lawfully Authorized and Conducted

In addition to challenging the general constitutionality of Section 702, the defendant questions the government's compliance with the applicable procedures with respect to the specific information that the government intends to use in this case. This Court's *in camera*, *ex parte* review of the relevant classified materials will establish that the collection at issue was lawfully authorized and conducted. To begin with, the applicable certifications and procedures, which were reviewed and approved by the FISC, complied with all of Section 702's requirements. Moreover, the Section 702 collection at issue was conducted in accordance with the statute and those approved certification(s) and procedures. *See* Part V., *infra*. Finally, although the defendant does not expressly challenge the information obtained or derived from physical search pursuant to Title III of FISA (traditional FISA), that information was also lawfully acquired and handled. *See* Part VI., *infra*.

3. The Defendant's Motions for Additional Notice and Discovery Should Be Denied

The defendant's motions for additional notice and discovery concerning other forms of surveillance lack merit and should be denied. The government has fully complied with its discovery obligations under F.R.C.P. 16, *Brady* and *Giglio*, and it has provided the defendant with all the notice to which he is entitled under FISA. *See* Part VII., *infra*. The defendant's speculation about the possibility he might have been

subject to other forms of collection fails to support his requests for additional disclosures. *See id.*

II. BACKGROUND

A. FACTUAL BACKGROUND⁸

1. Defendant Aws Mohammed Younis Al-Jayab

Defendant Aws Mohammed Younis Al-Jayab came to the United States as a United Nations refugee in October 2012 through an application filed by defendant's father Mohammed Younis Al-Jayab on behalf of his family. *See United States v. Aws Mohammed Younis Al-Jayab*, 16 CR 08 (E.D. Cal.), Doc. 1 at 2. At the time, the defendant was living with his family in a refugee camp in Syria. *Id.*

2. The Defendant's Plans to Travel to Syria

From the moment he arrived in the United States, the defendant began to plot his return to Syria to fight on behalf of terrorist groups there. *Id.* at 4-5. Beginning as early as mid-October 2012, via his Facebook accounts, the defendant told multiple family members and associates that he intended to travel to return to Syria to "work,"⁹ identified Turkey as a probable transit point, and sought to arrange the finances and logistics for his travel.¹⁰ *Id.* at 4.

⁸ [CLASSIFIED MATERIAL REDACTED]

⁹ Based upon the tenor and content of the defendant's extensive electronic communications, and the training and experience of the investigating agents, the government believes the term "work" referred to assisting and supporting violent jihad.

¹⁰ The messages referenced in this section were obtained via F.R.C.P. 41 search warrants and are primarily from the defendant's Facebook account with an identification number ending in 8752, with some messages from the defendant's Facebook account with an identification number ending in 6081.

On October 13, 2012, the defendant told an associate located in Iraq,¹¹ “I want to go back. . . I’ll go to Turkey and enter smuggled to Syria . . . When I come, I’ll call. Don’t go with anyone except the Front. [...] Go with Ansar or with the Front¹² only.”¹³ A couple of weeks later, on October 30, 2012, the defendant told an associate located in Syria that his trip to Syria would be expensive, and that he needed help from an individual named Khattab to enter Syria from Turkey. *Id.* at 5. The next day, the defendant was informed that Khattab would get the defendant into Syria from Turkey. *Id.*

A few months later, on January 20, 2013, the defendant exchanged Facebook messages with an individual known as Sayf, who was in Syria. *Id.* During that discussion, the defendant again noted that he needed money to travel to Syria, and Sayf told the defendant that Khattab would send him the money. *Id.* Sayf also wrote that he was afraid that he would die and not see the defendant and explained he (Sayf) had been shot twice in the hand and side. The defendant wrote, “I have someone in

¹¹ The locations of the individuals listed in this Section are based upon the investigating agents’ analysis of these individuals’ communications with defendant. That analysis is based on the content or context of the communications, the location posted on the individual’s social media page, the country and area code of the phone number provided, or other information gleaned from the communication.

¹² Based upon the training and experience of the investigating agents and the communications themselves, the government believes “Ansar” refers to Ansar Al-Islam, also known as Ansar Al-Sunna among other aliases, which is a Sunni terrorist group that has vowed to establish an independent Islamic state in Iraq; and “Front” refers to Al Nusra Front, also known as Jabhat Al Nusra. Ansar Al-Islam originated in Iraqi Kurdistan and was founded by Mullah Krekar. Pursuant to Section 219 of the Immigration and Nationality Act (“INA”), the U.S. Secretary of State designated Ansar Al Islam and Al Nusra Front as foreign terrorist organizations in 2004 and 2014, respectively. See www.state.gov/j/ct/rls/other/des/123085.

¹³ The translations of the communications detailed in this motion were based upon preliminary, and not final, translations of the Arabic-language communications.

Turkey. He wants to come to Syria and pull the trigger. Do you understand? Via the Turkish borders. [...] Tell Khattab about him.” Sayf told the defendant to let Sayf and Khattab know how much money the defendant needed so they could plan for his arrival in Syria and that Khattab could send the money. *Id.*

On February 1, 2013, the defendant asked a different individual for money and assistance in arranging his travel to Syria and in response was told to contact an individual known as Saqr. *Id.* at 5-6. A few days later, on February 5, 2013, Saqr, who was located in Syria, told the defendant via Facebook that Saqr would “go to Damascus to transfer the money to you,” and provided wire transfer details to defendant. *Id.* at 6. Later the same day, Saqr sent the defendant \$231 from Damascus, Syria, via Western Union. *Id.* Saqr also sent \$450 to one of the defendant’s associates, who, along with the defendant, was then residing in Arizona. *Id.* Both wire transfers were received at a Western Union in Arizona. *Id.* Two days later, the defendant confirmed with Saqr that he had received the combined \$681. *Id.*

Over a month later, on March 13, 2013, Saqr instructed the defendant via Facebook to “come to Turkey without a passport and enter Aleppo from there. Tell them you are Syrian.” The defendant and Saqr discussed various travel routes to Syria, and Saqr advised that he knew someone in Aleppo that Saqr had asked to assist the defendant. *Id.*

Soon thereafter, on March 23, 2013, the defendant wrote Facebook messages about his travel plans, how to best get into Syria through Turkey, and his plans to join the Jabhat Al-Nusra terrorist organization. *Id.* at 6-7. He told one individual, who

was in Iraq, that he was coming to Syria and that they should only work with the Jabhat Al-Nusra group. *Id.* at 6. The defendant told another individual known as Wissam Jamel, who was in Turkey, that he needed Wissam to pick him up at the airport. *Id.* at 7. Wissam asked if the defendant “want[ed] Al-Nusra Front,” referring to the same terrorist organization but using a different name, and the defendant responded, “that’s for sure.” *Id.* Wissam advised, “Syria is one hour away from where I am now and smuggling takes place in our area.” *Id.* When the defendant told Wissam that he would be traveling to Turkey with a United States travel document, Wissam reminded the defendant that it was important to maintain the ability to travel legally. *Id.* The defendant proposed, “I’ll go to the American Embassy in Turkey. I will tell them that due to circumstances, I can’t return now. . . I’ll say tourism, or I’ll tell him my grandmother is sick in Turkey and I wanted to be with her.” *Id.*

In April 2013, the defendant and Omar Al-Hardan, who resided in Texas,¹⁴ discussed via Facebook their plans to travel to Syria to fight with the mujahidin,¹⁵ and the defendant’s prior experience fighting in Syria. *Id.* at 7. The defendant explained that he had joined the mujahidin in Syria when he was 16 years old; and he fought for a group now known as Ansar Al-Islam, a designated terrorist organization. *Id.* at 10. During one conversation, the defendant said he had previously fought in Syria during a

¹⁴ On January 6, 2016, Al-Hardan was charged in the Southern District of Texas with one count each of providing material support to the Islamic State of Iraq and the Levant (“ISIL”), in violation of 18 U.S.C. § 2339B, procurement of citizenship or naturalization unlawfully, in violation of 18 U.S.C. § 1425(a), and making false statements, in violation of 18 U.S.C. § 1001. *See United States v. Omar Al Hardan*, 16 CR 03 (S.D. Tex.), at Doc. 1. On October 17, 2016, Al-Hardan pled guilty to the Section 2339B count. *Id.*, at Doc. 91.

¹⁵ A mujahidin is defined in the Merriam-Webster dictionary as an Islamic guerrilla fighter, especially in the Middle East.

battle against Syrian President Bashar al-Assad, adding, “God willing, you will have your chance to shoot . . . the most shots I made with it in my life was in the biggest battle I participated in. Seven magazines in one breath . . . Just shooting, spraying, spraying.” *Id.* at 9.

The defendant and Al-Hardan continued their discussions of firearms, referencing specific models like the PKC, GC, Glock, M16, and Kalashnikov. *Id.* at 7-9. Al-Hardan expressed his desire to learn from the defendant’s expertise with weapons, explaining that he had never “sprayed fire with a Kalashnikov.” *Id.* at 7, 9. The defendant responded:

Brother, God willing, you will be bored of shooting with guns. I have not seen anything better than the Glock. All my work was with the Glock and a nine Tariq and also its silencer. . . Once it hits someone, you would think the person fainted right before your eyes. It does not look like you killed him.

Id. at 9.

During another discussion about the defendant’s time fighting in Syria, Al-Hardan asked what “Assad’s soldiers scream when you raid?” and the defendant replied:

They fall silent. They stiffen. I remember once I went down together with a brother. We executed [...] three. As for the brother who was with me, he shot two. The third one aimed the Russian at the brother [...] and would not unlock the safety. He was so scared, he could not do it.

Id. The defendant continued:

Do you remember the national security headquarters building in Syria? The mujahidin, Al-Nusra Front struck it. [...] Those suicide bombers they want to break in. There is a control checkpoint that would stop them. Their car is full of

ammunition and suicide vests, its booby traps were visible, so they would stop them and arrest them. We got down and overran the control checkpoint and opened the way for them to raid, and we retreated.

Id. Al-Hardan then asked: "You mean you were there during the raid?" The defendant replied, "Yes. Look, God is with the mujahidin." *Id.*

Al-Hardan also sought guidance from the defendant regarding what would happen when they arrived in Syria. *Id.* 7-8. The defendant promised to train Al-Hardan and submit a request that he work for the defendant. *Id.* at 8. In another message to Al-Hardan, the defendant expressed his commitment to jihad, writing, "O God, grant us martyrdom for your sake while engaged in fighting and not retreating; a martyrdom that would make you satisfied with us." *Id.*

On April 16, 2013, the defendant wrote to a mujahidin in Syria via Facebook. The mujahidin told the defendant that he was in Damascus, but "also work[ed] in Jirmanah."¹⁶ Defendant said he was coming to Syria. *Id.* The mujahidin told the defendant that "we just killed ten of the Syrian militia, the Shabihah. Hahaha, with an IED [improvised explosive device]." *Id.* The defendant responded, "I was told that you and I will work together," adding, "I wish, come, let us do the killing together" and that he was "eager to see blood." *Id.*

In May 2013, the defendant learned that three of his associates were arrested by the Syrian government and accused of working for Al-Nusra Front. *Id.* at 10. The defendant ultimately told Al-Hardan about the arrests, and explained that he delayed

¹⁶ Jirmanah is a suburb or neighborhood of Damascus, Syria.

sharing this news because he “did not want you to feel uneasy about Jihad and be concerned with being detained.” *Id.*

From June through August 2013, the defendant continued to write to different associates about his travel preparations. *Id.* at 10-11. On June 30, 2013, the defendant said he was at a shooting club to learn long-range shooting, and shared photos of himself at a gun range in Wisconsin as well as photos of himself holding various weapons. *Id.* at 10. He wrote often about his need to raise money for his travel to Syria, and sought assistance in planning his route. *Id.* at 10-11. Notably, during this time period, the defendant communicated with Abu ‘Akkab al-Muhajir (al-Muhajir), who was based in Syria and used his Facebook account to distribute propaganda for the Islamic State of Iraq and the Levant (“ISIL”) and communicate with individuals affiliated with ISIL and other terrorist organizations.¹⁷ *Id.* at 11.

As the months passed, the defendant grew increasingly desperate to get to Syria. *Id.* On September 8, 2013, the defendant told Sayf, “I am burning with desire to come there and work.” *Id.* They then discussed a photo of various weapons including a gray gun and Kalashnikov rifle that Sayf claimed were his firearms. *Id.* Sayf promised, “When you arrive here, we will give you better ones [...] along with five magazines, one of which holds 30,” meaning 30 rounds of ammunition. The defendant replied, “I wish you will not die until I come.” *Id.*

¹⁷ In 2004, pursuant to Section 219 of the INA, the U.S. Secretary of State designated al-Qaeda in Iraq as a foreign terrorist organization. In 2014, the Secretary of State amended that foreign terrorist organization designation to add the alias “Islamic State of Iraq and the Levant” (“ISIL”) as its primary name, along with additional aliases for ISIL. See www.state.gov/j/ct/rls/other/des/123085.

On October 29, 2013, al-Muhajir promised the defendant that he had tasked Sayf with getting defendant the money he needed to travel to Syria. *Id.*

3. The Defendant's Travel to Turkey and Syria

In early November 2013, when the defendant was residing in the Milwaukee, Wisconsin, area, he received approximately \$4,500 in an insurance settlement. On November 7, 2013, the defendant told al-Muhajir that he would use the money to travel to Turkey, and needed al-Muhajir to make arrangements for his travel from there to Syria. *Id.* at 12. The next day, the defendant purchased an airline ticket, and on November 9, 2013, flew directly from Chicago to Istanbul, Turkey. *Id.*

From there, the defendant traveled to Syria. The FBI confirmed the defendant's presence in Syria from November 2013 through January 2014 using two types of information. First, investigating agents reviewed the Internet Protocol ("IP") addresses that the defendant used during that time to connect to the internet to access Facebook and e-mail accounts. *Id.* Analyses of those IP addresses and related information established that the defendant accessed the internet during the relevant time period through a satellite that covered both eastern Turkey and areas of northern Syria. *Id.*

Second, the content of the defendant's communications consistently referenced his presence in Syria during this timeframe. For example, on November 10, 2013, the defendant told his brother Younis, who was then residing in Cyprus, that the defendant was in Turkey, planned to enter Syria, and would be "going with the Mujahidin." *Id.* About ten days later, the defendant confirmed that he had safely

arrived in Aleppo, a Syrian city. *Id.* On November 26, 2013, the defendant told al-Muhajir that he was in Aleppo and gave al-Muhajir his Syrian telephone number. *Id.* at 12-13.

Indeed, a number of the defendant's conversations with Younis revolved around Younis' concerns that the defendant was revealing his presence in Syria when he used his phone. On November 28, 2013, Younis told the defendant to avoid using his phone because it showed "that [defendant was] writing from Aleppo." *Id.* at 13. Younis wrote, "Aws, I need you to get out of Syria as soon as possible" and noted the defendant's phone "will reveal that you are in Syria [...] and this is dangerous to your situation over there." *Id.* A couple of weeks later, on December 10, 2013, Younis again informed the defendant, "It shows that you are typing from Al-Hasakah," a city in northeastern Syria. *Id.* Shortly thereafter, the defendant replied, "Forgive me, I might become a martyr." *Id.*

The defendant and Younis engaged in additional conversations that further demonstrated that the defendant was armed while in Syria. For example, on December 23, 2013, the defendant wrote, "I have m16," meaning an M16 assault rifle. *Id.* Soon thereafter Younis told the defendant to remove a picture from Facebook that "shows that you are wearing military uniform." *Id.*

The defendant knew his travel to Syria to fight with a terrorist organization was illegal. In an early December 2013 message to Younis, he wrote that he was "afraid of being imprisoned in America [because] the government is alert for everything, [and] my trip here constitutes a charge." *Id.*

Despite these fears, the defendant continued to work with terrorist organizations. On December 28, 2013, the defendant told an associate that he was in Aleppo and had joined Ansar al-Sham, which he explained was “the same as Ansar al-Islam, just with another name.” *Id.* at 13-14. The defendant continued, “It is the one that leads the new Islamic Front formed after merging with Jabhat al-Nusra,” but he noted that this alliance had not been publicly declared. *Id.* at 14. The defendant further explained, “The Army of Islam and Ahrar al-Sham and Al-Tawhid Brigade became the al-Jabhah al-Islamiyyah.”¹⁸ When they engage in battles [they are] led by Jabhat al-Nusra and Ansar al-Sham.” *Id.* The defendant detailed the cooperation and “joint action” that existed between certain Sunni extremist groups engaged in the conflict against the Syrian regime. *Id.*

The defendant also expressed his concern over conflict that was occurring amongst some of the Islamic groups in the area. He wrote that ISIL, which he referred to as “the State,” “have killed many from Jabhat al-Nusra and hundreds of mujahidin [are detained] by the State . . . Brother, this is the blood of Muslims shed at the hands of the State.” He continued:

If it weren't for the State's bloodletting, I would have been the first one to join it. [That's] why I joined the al-Ansar even though there's little action; the al-Ansar, at least they don't kill Muslims . . . Brother, I'll join al-Nusra shortly [...] and if any sedition arises, I'll leave my weapon and go to Turkey.

¹⁸ According to open source information, Al-Jabhah al-Islamiyyah is an Arabic phrase that translates to “the Islamic Front.” The Islamic Front was an umbrella organization of Sunni Salafist groups fighting to depose the Syrian regime. In late 2013, founding members of the Islamic Front included Ansar al-Sham, Ahrar al-Sham, the Tawhid Brigade, and the Army of Islam.

Id.

Despite these concerns, the defendant still expressed an interest in joining ISIL. In January 2014, he wrote “I have been thinking of joining the State and abandon[ing] the al-Ansar.” *Id.* The defendant explained that he was in “Haritan, Aleppo, a fighting zone [between] the State and the Free Army.”¹⁹ *Id.* at 15. When asked if he was with “the Free now,” meaning the Free Army, the defendant replied, “No. Ansar al-Islam.”

Id. The next day, the defendant wrote:

Brother, we do not sit and watch. [...] Our headquarters is next to the State exactly, and we are against the Free Army. We have prevented the Free Army from entering the area and attacking the State’s headquarters. And if the Free Army advances, we will fight it. [...] We installed the Doshkas [a Russian machine gun widely used in the Syrian conflict] in the street and spread among all of our headquarters because we are at the entrance of Aleppo. The Free Army is under the control of our forces.

Id.

Ultimately, as a result of these internal conflicts between the terrorist organizations, the defendant began to express his intention to return home. For example, on January 7, 2014, he wrote:

I swear that the State is killing [members of] al-Ansar and al-Nusra. They are our brothers, but they are making a mistake. And we are going to stand with the State against the [Free Army] . . . I might withdraw. . . . When the seditious acts are over, I will return. . . . I did not come to fight for the sake of sedition.

Id.

¹⁹ According to open source information, the Free Syrian Army was established in 2011 by Syrian military defectors, and it has since become an umbrella organization for various armed opposition groups fighting to depose the regime of President al-Assad.

4. The Defendant's Return to Turkey and the United States

On January 8, 2014, the defendant told his brother Younis that the border crossing with Turkey was closed and defendant remained in Aleppo. *Id.* On January 17, 2014, the defendant informed an associate that he would "leave in two hours . . . Once I arrive in Turkey I will call you." *Id.* at 16. Several hours later that day, the defendant's Facebook account was accessed from an IP address in Turkey. *Id.*

Travel records confirm that the defendant flew to Sacramento, California, via London and Los Angeles on January 23, 2014.²⁰ *Id.* Upon his return to the United States, the defendant made no mention of his travel to Turkey and Syria on his Customs Declaration Form; he listed only "Jordan" and "U.K." in the form's "countries visited" field. *Id.*

5. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

6. USCIS and FBI Interviews

On July 29, 2014, the defendant was interviewed by employees of the U.S. Citizenship and Immigration Services ("USCIS") as part of his application for adjustment of his immigration status. *Id.* During that interview, which was audio-recorded, the defendant said he had traveled to Turkey about six months earlier, which was January 2014. *Id.*

²⁰ The defendant had never lived in Sacramento, California, before he returned from Syria in January 2014.

On October 6, 2014, the defendant was interviewed by USCIS employees a second time. *Id.* at 17. In this audio-recorded interview, the defendant denied any terrorist affiliations and falsely represented that he traveled to Turkey to visit his grandmother. *Id.* Based on interviews with the defendant's family members conducted after defendant's arrest, the defendant does not have a grandmother living in Turkey. *Id.*

On June 18, 2015, the defendant was interviewed by FBI agents after he requested to meet with them regarding problems he experienced at the airport when traveling. *Id.* at 16. During that interview, the defendant stated that he had traveled to Turkey for a vacation in 2014. *Id.* He denied traveling to Syria in 2013 or 2014. *Id.*

B. CHARGES AND PROCEDURAL HISTORY

[CLASSIFIED MATERIAL REDACTED]

On January 7, 2016, the defendant was arrested in the Eastern District of California pursuant to a federal criminal complaint filed in that district. *See Al-Jayab*, 16 CR 08 (E.D. Cal.), Doc. 1. The complaint charged the defendant with knowingly providing a materially false statement to federal agents in a matter involving international terrorism, based on the false statement defendant made to the USCIS employees on October 6, 2014, in violation of 18 U.S.C. § 1001. *Id.* On January 14, 2016, a grand jury sitting in the Eastern District of California returned a one-count indictment charging this offense. *Id.*, Doc. 13.

On March 17, 2016, a one-count indictment was filed in this Court, charging the defendant with attempting to provide material support to terrorists, in violation of 18

U.S.C. § 2339A. Doc. 1. On April 8, 2016, pursuant to 50 U.S.C. §§ 1825(d) and 1881e(a), the United States provided notice to the defendant that it “intends to offer into evidence, or otherwise use or disclose in any proceedings in this matter, information obtained or derived from physical searches and acquisitions acquired pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, Title 50, United States Code, Sections 1821-1829 and 1881a.” (Doc. 14). The defendant, who has been detained since his arrest and initial appearance, was transferred to Chicago to appear on the material support charge. The two cases are proceeding simultaneously. The trial in the instant case is scheduled to begin on February 12, 2018. No trial has been scheduled yet in the Eastern District of California. The defendant filed his motion to suppress, supporting memoranda, and related motions on March 14, 2017. (Docs. 48-52.)

C. OVERVIEW OF THE SECTION 702 COLLECTION AT ISSUE

[CLASSIFIED MATERIAL REDACTED]

III. OVERVIEW OF FISA AND THE FISA AMENDMENTS ACT

A. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

In 1978, Congress enacted FISA “to regulate the use of electronic surveillance within the United States for foreign intelligence purposes.” *See* S. Rep. No. 95-604, at 7 (1977). Before the United States may conduct “electronic surveillance,” as defined in FISA, to obtain foreign intelligence information, the statute generally requires the

government to obtain an order from a judge of the FISC.²¹ See 50 U.S.C. § 1805; see 50 U.S.C. §§ 1803(a), 1804(a). To obtain such an order, the government must establish, *inter alia*, probable cause to believe that the “target of the electronic surveillance is a foreign power or an agent of a foreign power” and that “each of the facilities or places at which the electronic surveillance is directed” (inside or outside the United States) “is being used, or is about to be used, by a foreign power or an agent of a foreign power.” 50 U.S.C. § 1805(a)(2). The government must also establish that the “minimization procedures” that it will employ are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublic information concerning unconsenting “United States persons,” consistent with the government’s need to obtain, produce, and disseminate foreign intelligence information. See 50 U.S.C. §§ 1801(h), 1805(a)(3) and (c)(2)(A).

Under FISA as originally enacted, only “electronic surveillance” was subject to the requirement of a judicial order based on probable cause. FISA’s original “electronic surveillance” definition did not apply to most of the government’s extraterritorial surveillance.²² This was true even if that surveillance might specifically target U.S.

²¹ The judges of the FISC are Article III judges who serve by designation of the Chief Justice of the United States. See 50 U.S.C. § 1803(a).

²² In FISA, Congress defined “electronic surveillance” to include four discrete types of domestically-focused foreign intelligence collection activities: (1) the acquisition of the contents of a wire or radio communication obtained by “intentionally targeting” a “particular, known United States person who is *in the United States*” in certain circumstances; (2) the acquisition of the contents of a wire communication to or from a “person *in the United States*” when the “acquisition occurs in the United States”; (3) the intentional acquisition of the contents of certain radio communications when the “sender and all intended recipients are located *within the United States*”; and (4) the installation or use of a surveillance device “*in the United States*”

persons abroad or incidentally acquire, while targeting third parties abroad, communications to or from U.S. persons or persons located in the United States. *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., at 7 & n.2, 34-35 & n.16 (1978).²³ At the time of FISA's enactment, the acquisition of international communications did not rely on the four types of "electronic surveillance" covered by the definitions in the proposed legislation—including wire interceptions executed in the United States—and thus those operations would not be affected by FISA. *See Foreign Intelligence Surveillance Act: Hearings on S. 743, S. 1888, and S. 3197 Before the Subcomm. on Crim. Laws and Procedures of the S. Judiciary Comm., 94th Cong., 11 (1976)*. Accordingly, at the time FISA was enacted, Congress understood that most foreign-to-foreign and international communications fell outside the definition of "electronic surveillance." *See* S. Rep. No. 95-701 at 71 ("[T]he legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency."). Where the government did not intentionally target a particular, known U.S. person in the United States, FISA allowed the government to monitor international communications through radio surveillance, or wire surveillance of transoceanic cables offshore or on foreign soil, outside the statute's regulatory framework.

for monitoring or to acquire information other than from a wire or radio communication in certain circumstances. 50 U.S.C. § 1801(f) (emphasis added).

²³ Executive Order 12333, as amended, addresses, *inter alia*, the government's "human and technical collection techniques . . . undertaken abroad." Exec. Order No. 12333, § 2.2, 3 C.F.R. § 210 (1981 Comp.), *reprinted as amended in* 50 U.S.C. § 401 note (Supp. II 2008).

B. THE PROTECT AMERICA ACT

By 2007, many international communications that would have been generally excluded from FISA regulation in 1978, when they were carried by radio, were now transmitted principally by fiber optic cables and therefore qualified as wire communications under FISA. *Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intel.*, 110th Cong., 19 (2007) (Statement of Admiral J. Michael McConnell, USN, Ret., Director of National Intelligence) (“May 1, 2007 FISA Modernization Hrg.”). Once that change occurred, FISA potentially regulated the surveillance of international communications that were previously not covered by the statute, due merely to a change in technology rather than any intentional legislative decision. *Id.*²⁴

The government in 2007 thus faced a different communications technology environment and a different terrorist threat and needed greater flexibility than the statute’s terms allowed.²⁵ The fix needed, as a Department of Justice official stated,

²⁴ Compare 50 U.S.C. § 1801(f)(2) (defining wire communication as “electronic surveillance” if, *inter alia*, one party is in the United States) with 50 U.S.C. § 1801(f)(3) (defining radio communication as “electronic surveillance” only if the sender and all intended recipients are in the United States).

²⁵ As the DNI testified:

In today’s threat environment, . . . FISA . . . is not agile enough to handle the community’s and the country’s intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. – that is, foreign – persons located outside the United States This clogs the FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

May 1, 2007 FISA Modernization Hrg. 18.

was a “technology-neutral” framework for surveillance of foreign targets—focused not on “how a communication travels or where it is intercepted,” but instead on “who is the subject of the surveillance, which really is the critical issue for civil liberties purposes.” May 1, 2007 FISA Modernization Hrg. 46 (statement of Asst. Att’y Gen. Kenneth L. Wainstein).

In August 2007, Congress enacted the Protect America Act (“PAA”), Pub. L. No. 110-55, 121 Stat. 552 (2007), to bring FISA “up to date with the changes in communications technology” and address “degraded capabilities in the face of a heightened terrorist threat environment,” while at the same time preserving “the privacy interests of persons in the United States.” S. Rep. No. 110-209, at 5-6 (2007) (internal quotation marks omitted). The PAA fulfilled these purposes by permitting the Attorney General and the DNI to jointly authorize “the acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States.” 50 U.S.C. § 1805b(a). To authorize such collection, the PAA required the Attorney General and the DNI to certify, *inter alia*, that there were reasonable procedures in place for determining that the acquisition concerned persons (whether U.S. persons or non-U.S. persons) reasonably believed to be located outside the United States (“targeting procedures”), there were minimization procedures in place that satisfied FISA’s requirements for such procedures, and a significant purpose of the acquisition was to obtain foreign intelligence information. *See* 50 U.S.C. § 1805b(a)(1)-(5). The PAA also authorized the FISC to review the determination of the Attorney General and the DNI as to the reasonableness of the targeting procedures.

Finally, the PAA allowed private parties who had been directed by the government to assist in effectuating acquisitions under the statute to challenge the legality of the directive before the FISC, *see id.* § 1805b(h)(1)(A), and to appeal an adverse decision to the Foreign Intelligence Surveillance Court of Review (“FISA Court of Review”), *see id.* § 1805b(i). One party brought such a challenge, and both the FISC and the FISA Court of Review upheld the PAA. *See In re Directives Pursuant to Section 105B of FISA*, 551 F.3d 1004 (FISA Ct. Rev. 2008).

C. THE FISA AMENDMENTS ACT OF 2008

Pursuant to a sunset provision, the PAA expired in February 2008. In July 2008, Congress enacted the FAA, which included a new Section 702 of FISA.²⁶ Section 702 (50 U.S.C. § 1881a) “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 v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1144 (2013).²⁷ Section 702 provides that, “upon the issuance” of an order from the FISC, the Attorney General and DNI may jointly authorize the “targeting of persons²⁸ reasonably believed to be located

²⁶ In 2012, Congress reauthorized the FAA for an additional five years. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

²⁷ The FAA enacted other amendments to FISA, including provisions not at issue in this case that govern the targeting of United States persons outside the United States. *See* 50 U.S.C. §§ 1881b, 1881c.

²⁸ A “person” under Section 702 includes an individual, group, entity, association, corporation, or foreign power as defined under the statute. 50 U.S.C. §§ 1801(m), 1881(a). “Person” under FISA, however, cannot include an entire geographic region or foreign country. *See* Privacy and Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 20-21 (July 2, 2014), available at <http://www.pclob.gov/library/702-Report.pdf> (“PCLOB Report”). The PCLOB is an independent

outside the United States” for a period of up to one year to acquire “foreign intelligence information.” 50 U.S.C. § 1881a(a).²⁹ In accordance with the statutory limitations discussed below, Section 702 only authorizes the targeting of persons who are both non-U.S. persons and reasonably believed to be located overseas to acquire foreign intelligence information as defined by the statute.

Under Section 1881a(b), the authorized acquisition must comply with each of the following requirements, which are directed at preventing the intentional targeting of U.S. persons or persons located within the United States (whether they are U.S. persons or non-U.S. persons), or the collection of communications known at the time of acquisition to be purely domestic:

(1) The authorized acquisition “may not intentionally target any person known at the time of acquisition to be located in the United States.” 50 U.S.C. § 1881a(b)(1).

(2) It may not intentionally 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).

agency within the Executive Branch established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. No. 110-53, and signed into law in August 2007. The PCLOB was tasked by a bipartisan group of U.S. Senators to investigate Section 702, among other authorities, and to issue an unclassified report. As part of its investigation, the PCLOB held public hearings and reviewed classified information provided by the Intelligence Community, some of which was declassified for use in the PCLOB report. PCLOB Report at 1-3. The PCLOB concluded 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”—is reasonable under the Fourth Amendment. *Id.* at 9.

²⁹ The Attorney General and DNI may authorize targeting to commence under Section 702 before the FISC issues its order if they determine that certain “exigent circumstances” exist. 50 U.S.C. § 1881a(a), (c)(2). If that determination is made, the Attorney General and DNI must, as soon as practicable (and within seven days), submit for FISC review their Section 702 certification, including the targeting and minimization procedures used in the acquisition. 50 U.S.C. § 1881a(g)(1)(B); *see* 50 U.S.C. § 1881a(d), (e), (g)(2)(B).

(3) It “may not intentionally target a United States person reasonably believed to be located outside the United States.” 50 U.S.C. § 1881a(b)(3).

(4) It “may not intentionally acquire 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(b)(4).

(5) The acquisition must be “conducted in a manner consistent with the [F]ourth [A]mendment.” 50 U.S.C. § 1881a(b)(5).

Section 702 does not require an individualized court order addressing each non-U.S. person to be targeted under its provisions. Section 702 instead permits the FISC to approve annual certifications by the Attorney General and DNI that authorize the acquisition of certain categories of foreign intelligence information – such as information concerning international terrorism and the acquisition of weapons of mass destruction – through the targeting of non-U.S. persons reasonably believed to be located outside the United States.³⁰ See PCLOB Report at 25 & n.71 (citing public

³⁰ The categories of information being sought under a certification must meet FISA’s definition of foreign intelligence information:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against --

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to -

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also* 50 U.S.C. § 1881(a).

statements by the General Counsels of the Office of the Director of National Intelligence ("ODNI"), NSA, and FBI).

1. The Government's Submission to the FISC

Section 702 requires the government to obtain the FISC's approval of (1) the government's certification regarding the proposed collection, and (2) the 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), (g)(2)(B). The Attorney General and DNI must certify that:

(1) there are targeting procedures in place, that have been or will be submitted for approval by the FISC, that are reasonably designed to ensure that the acquisition is limited to targeting persons reasonably believed to be located outside the United States and to prevent the intentional acquisition of purely domestic communications;

(2) the minimization procedures meet the definition of minimization procedures set forth in Titles I and III of FISA (50 U.S.C. §§ 1801(h), 1821(4)) and have been or will be submitted for approval by the FISC;

(3) guidelines have been adopted by the Attorney General to ensure compliance with the aforementioned limitations set forth in Section 1881a(b) prohibiting, among other things, the targeting of United States persons;

(4) the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment;

(5) a significant purpose of the acquisition is to obtain foreign intelligence information;

(6) the acquisition involves obtaining "foreign intelligence information from or with the assistance of an electronic communication service provider"; and

(7) the acquisition complies with the limitations in Section 1881a(b).³¹

50 U.S.C. § 1881a(g)(2)(A)(i) - (vii); *see* 50 U.S.C. §§ 1801(h), 1821(4), 1881a(b); *cf.* 50 U.S.C. §§ 1801(e), 1881(a) (defining “foreign intelligence information”). Such certifications are “not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under [section 1881a(a)] will be directed or conducted.” 50 U.S.C. § 1881a(g)(4).

The certification must include copies of the targeting and minimization procedures, and a supporting affidavit, “as appropriate,” from the head of an Intelligence Community element or other Senate-confirmed official “in the area of national security.” 50 U.S.C. § 1881a(g)(2)(B) - (C). Finally, the certification must include “an effective date for the authorization that is at least 30 days after the submission of the written certification” to the FISC. 50 U.S.C. § 1881a(g)(2)(D)(i).

[CLASSIFIED MATERIAL REDACTED]

2. The FISC’s Order(s) and Opinion(s)

The FISC must review the certification, targeting and minimization procedures, and any amendments thereto. 50 U.S.C. § 1881a(i)(1) and (2). If the FISC determines that the certification contains all the required elements and concludes that the targeting and minimization procedures and the Attorney General guidelines for compliance with the statutory limitations are “consistent with” both the Act and “the [F]ourth [A]mendment,” the FISC will issue an order approving the certification and

³¹ Those limitations, as described above, generally prevent the intentional targeting of United States persons or persons located within the United States or collection of communications known at the time of acquisition to be purely domestic.

the use of the targeting and minimization procedures. 50 U.S.C. § 1881a(i)(3)(A). If the FISC finds deficiencies in the certification or procedures, it must issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any deficiency within 30 days, or cease or not begin implementation of the authorization. 50 U.S.C. § 1881a(i)(3)(B).

[CLASSIFIED MATERIAL REDACTED]

3. Implementing Section 702 Authority

The government acquires communications pursuant to Section 702 through compelled assistance from electronic communications service providers. 50 U.S.C. § 1881a(h). The government identifies to these service providers specific communications facilities (also referred to as “selectors”), such as e-mail 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 abroad, (2) who possess, communicate, or are likely to receive a type of foreign intelligence information authorized for collection under a FISC-approved certification. See PCLOB Report at 32-33, 41-46.

Once a selector has been tasked for acquisition pursuant to FISC-approved targeting procedures, acquisition against that selector is compelled through a directive served on a provider. There are two types of Section 702 acquisition: “PRISM” collection and “upstream” collection. See PCLOB Report at 33. In “PRISM” collection, the government sends a selector to a service provider who is compelled by the directive to provide to the government communications sent either to or from that selector

(known as “to/from” communications). *Id.* “Upstream” collection involves telephony and Internet data acquisitions conducted with the compelled assistance of the providers that control the telecommunications backbone within the United States over which communications transit. *Id.* at 35. It includes the collection of to/from communications, and, until recently, also involved the collection of certain communications referring to the particular selector (for example, a targeted e-mail address in the body of the e-mail) known as “about” communications.³² *Id.* at 37.

This case does not involve “upstream” collection.³³ Accordingly, the lawfulness of upstream collection is not at issue here.³⁴ *See In re Directives*, 551 F.3d at 1010 (where “a statute has been implemented in a defined context, an inquiring court may only consider the statute’s constitutionality in that context”); *see also United States v.*

Mohamud, 843 F.3d 420, 438 (9th Cir. 2016) (“*Mohamud II*”) (declining to address

³² *See [Caption Redacted]*, 2011 WL 10945618, at *6 n.16 (FISA Ct. Oct. 3, 2011) (“[A]ll ‘about’ communications are acquired by means of NSA’s acquisition of Internet transactions through its upstream collection.”); *see also* Mem. Op. and Order at 26, *[Caption Redacted]* (FISA Ct. Apr. 26, 2017) (“*April 2017 FISC Op.*”) (noting that the government has ceased collection of “about” communications), available at https://www.dni.gov/files/documents/icotr/511117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

³³ [CLASSIFIED MATERIAL REDACTED]

³⁴ Thus, the defendant’s arguments regarding “about” communications and upstream collection (*see* Doc. 48 at 18, 19-20, 31, 33, 43) are not relevant to the Court’s consideration of the constitutionality of Section 702 as it was implemented in this case. Similarly irrelevant is the portion of the declassified 2011 FISC opinion, referenced in the defendant’s motion (*see* Doc. 48 at 23-24 n.21, 33), in which the FISC concluded that the NSA’s minimization procedures were deficient with respect to the retention of certain upstream acquisitions (those including “Multi Communication Transactions” or “MCTs”). *See [Caption Redacted]*, 2011 WL 10945618, at *9-28. It also should be noted that the government promptly revised the NSA minimization procedures and thus cured the deficiency identified by the FISC. *See [Caption Redacted]*, 2011 WL 10947772, at *1 (FISA Ct. Nov. 30, 2011) (holding that revised procedures were consistent with statutory requirements and the Fourth Amendment). *See also April 2017 FISC Op.* at 15-30 (discussing issues with upstream collection and recent narrowing of such collection by government).

lawfulness of upstream collection and instead limiting review “to the particular facts of this case”).

4. Targeting and Minimization Procedures

The government may conduct acquisitions under Section 702 only in accordance with specific targeting and minimization procedures that are subject to review and approval by the FISC. 50 U.S.C. § 1881a(c)(1)(A), (d), (e), and (i)(3)(A). The targeting procedures must be reasonably designed to restrict acquisitions to the targeting of persons reasonably believed to be outside the United States and applied using compliance guidelines to ensure that the acquisitions do not intentionally target U.S. persons or persons located in the United States. 50 U.S.C. §§ 1881a(b), (d)(1) and (f)(1)(A). The minimization procedures, in turn, must be reasonably designed to minimize any acquisition of nonpublicly available information about unconsenting U.S. persons, and to minimize the retention and to prohibit the dissemination of any such information that might nevertheless be acquired, consistent with the need to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. §§ 1801(h)(1), 1821(4)(A); *see* 50 U.S.C. § 1881a(e)(1).³⁵ The FISC must substantively review the targeting and minimization procedures to ensure that they satisfy the statutory

³⁵ Minimization procedures must also “allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.” 50 U.S.C. § 1801(h)(3). The definitions of minimization procedures in 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D), which apply only to electronic surveillance approved pursuant to 50 U.S.C. § 1802(a) and physical searches approved pursuant to 50 U.S.C. § 1822(a), respectively, do not apply to acquisitions conducted under Section 702.

criteria and are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(i)(2)(B), (C) and (3)(A).

The NSA, FBI, and CIA have separate sets of minimization procedures that govern each agency's retention and dissemination of information acquired through Section 702.³⁶ PCLOB Report at 51. Each set of minimization procedures takes into account the unique mission of the agency and the systems in which each agency stores and analyzes Section 702-acquired information.

[CLASSIFIED MATERIAL REDACTED]

a. Targeting Procedures

There are two agencies that conduct acquisitions under Section 702: the NSA and the FBI. Each agency conducts acquisitions pursuant to separate sets of targeting procedures. Other intelligence agencies can provide the NSA with "lead" information to initiate the collection from a selector. *See* PCLOB Report at 42; *see id.* at 47.³⁷

Once the NSA identifies a potential person to target through tasking a selector, the targeting procedures³⁸ require the NSA to assess whether the potential target is a non-U.S. person reasonably believed to be located outside the United States and whether the target possesses and/or is likely to communicate or to receive foreign

³⁶ The National Counterterrorism Center also is subject to minimization procedures, but its role in processing and minimizing Section 702 data is limited. *See* PCLOB Report at 51 n.215; *see also April 2017 FISC Op.* at 30-48.

³⁷ The PCLOB Report (*see* footnote 28, *supra*) provides a general, unclassified description of Section 702 targeting and minimization procedures. The following discussion of targeting and minimization procedures is derived from the PCLOB's description but also is supplemented, as indicated, with additional information concerning the particular procedures that were applied in this case, which are classified and have been filed under seal with the Court.

³⁸ **[CLASSIFIED MATERIAL REDACTED]**

intelligence information authorized under an approved certification. *See id.* at 43. The determination regarding the location and non-U.S. person status is based on the totality of the circumstances and cannot be based on lead information alone. *Id.*³⁹ If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting. *Id.* at 44. In making the foreign intelligence purpose determination, the NSA must identify the particular foreign power or foreign territory about which the government is seeking foreign intelligence information. *Id.* at 45.⁴⁰ The targeting procedures require documentation of the NSA's determinations. *Id.* at 45-46.⁴¹ In addition, tasking requests by NSA analysts undergo an internal approval process prior to a selector being tasked for acquisition and, as discussed below, are subject to additional review by external oversight teams with the Department of Justice and the ODNI. *Id.* at 46.⁴² Once the NSA has assessed that the potential target is a non-U.S. person located outside the United States and that targeting of the person is likely to result in the acquisition of foreign intelligence information, the NSA may task the facility used by the target pursuant to Section 702. *See id.*

After tasking, the NSA targeting procedures impose additional requirements designed to ensure that the users of tasked facilities remain non-U.S. persons located

³⁹ [CLASSIFIED MATERIAL REDACTED]

⁴⁰ [CLASSIFIED MATERIAL REDACTED]

⁴¹ [CLASSIFIED MATERIAL REDACTED]

⁴² [CLASSIFIED MATERIAL REDACTED]

outside the United States and that acquisition against the facility continues only insofar as the government assesses that the tasking is likely to acquire foreign intelligence information within an authorized Section 702 certification. *See id.* at 48-49.⁴³ The post-targeting analysis includes examining the content of communications obtained through surveillance of a tasked selector for indications that a targeted person had entered, or might soon enter, the United States. *See id.* at 48.⁴⁴ It also includes comparing each selector against independently acquired information for indications that a tasked selector may be used inside the United States. *See id.*⁴⁵

In the event that the NSA concludes that a target has entered the United States, or that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, the NSA must promptly detask all facilities used by the target from Section 702 acquisition. *Id.* at 49.⁴⁶ Selectors must also be detasked if the government determines that it will not obtain the types of foreign intelligence information authorized under the Section 702 certification(s). *Id.* Failure to detask a selector from Section 702 acquisition after it has been (or, based on available information, should have been) determined to be ineligible for Section 702 collection is a compliance incident that must be reported to the Department of Justice and ODNI. *Id.*⁴⁷ Any data acquired from a selector while it was being used by a U.S.

⁴³ [CLASSIFIED MATERIAL REDACTED]

⁴⁴ [CLASSIFIED MATERIAL REDACTED]

⁴⁵ [CLASSIFIED MATERIAL REDACTED]

⁴⁶ [CLASSIFIED MATERIAL REDACTED]

⁴⁷ [CLASSIFIED MATERIAL REDACTED]

person or a person in the United States is subject to purge, with limited exceptions. *Id.* at 49-50.

The FBI's targeting procedures govern certain aspects of PRISM collection, specifically requests for certain communications for selectors that have already been determined by the NSA to have met its targeting procedures. *Id.* at 47.⁴⁸ The FBI's targeting procedures are intended to "provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States." *See [Caption Redacted]*, 2011 WL 10945618, at *7. The targeting procedures therefore require the FBI both to review the NSA's determinations regarding the non-U.S. person status and overseas location of the target, and to review information available to the FBI. PCLOB Report at 47.

b. Minimization Procedures

As noted above, Section 702 also requires the adoption of minimization procedures that comply with FISA's definition of such procedures. *See* 50 U.S.C. § 1881a(e)(1). FISA-compliant minimization procedures are, in pertinent part:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information . . . , shall not be disseminated in a manner that identifies any United States person, without such person's

⁴⁸ [CLASSIFIED MATERIAL REDACTED]

consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

50 U.S.C. § 1801(h); *see also* 50 U.S.C. § 1821(4); 50 U.S.C. § 1801(e) (defining "foreign intelligence information"). All Section 702-acquired information is subject to the FISC-approved minimization procedures.

As a general matter, the minimization procedures of agencies that conduct Section 702 acquisitions (the NSA and FBI)⁴⁹ contain provisions that limit the acquisition of U.S. person information consistent with the authorized purpose of the collection. *See* PCLOB Report at 51-52. The minimization procedures for agencies that handle Section 702 collection (principally, the NSA, CIA and FBI) also contain limitations on the retention, use, and dissemination of U.S. person information acquired through Section 702 acquisitions. *Id.* at 53, 64. For example, each agency limits access to unminimized Section 702-acquired data to personnel who have been trained to apply the applicable minimization procedures. *See id.* at 53-54.⁵⁰ The minimization procedures also contain provisions regarding when unminimized data must be deleted from agency systems after specified periods of time and other provisions requiring that certain data be purged upon recognition. *See id.* at 60-63. The minimization procedures permit the dissemination of U.S. person information only

⁴⁹ [CLASSIFIED MATERIAL REDACTED]

⁵⁰ [CLASSIFIED MATERIAL REDACTED]

if any information that could identify the U.S. person is deleted, absent certain specific circumstances. Such circumstances may include where the U.S. person has consented to the dissemination, the specific information about the U.S. person is already publicly available, the U.S. person's identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities. *Id.* at 64-65.⁵¹

5. Oversight

Section 702 requires that the Attorney General and the DNI periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines, and that they submit those assessments both to the FISC and to Congressional oversight committees. 50 U.S.C. § 1881a(l). In addition, not less often than once every six months, the Attorney General must keep the relevant Congressional oversight committees "fully inform[ed]" concerning the implementation of Section 702. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment."). Such committees include the Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee. *See* PCLOB Report at 69.

The government's use of the Section 702 authorities is also subject to internal oversight by various entities within each agency that has a role in the acquisition,

⁵¹ [CLASSIFIED MATERIAL REDACTED]

retention, or dissemination of Section 702 information. *See id.* at 66-68. Moreover, incidents of non-compliance with the targeting or minimization procedures that are identified by any internal compliance efforts, or that are otherwise self-identified by the agencies, must be reported to the Department of Justice and ODNI. *Id.* at 68.

In addition, the FISC Rules of Procedure require the government to notify the FISC whenever the government discovers a material misstatement or omission in a prior filing with the court, including with respect to Section 702 certifications. *See, e.g., [Caption Redacted]*, 2011 WL 10945618, at *2. Rule 13(b) of the Rules of Procedures for the FISC requires the government to report, in writing, all instances of non-compliance. The government reports Section 702 compliance incidents to the FISC via individual notices and quarterly reports.⁵² *See* PCLOB Report at 75-76. The FISC has noted that it considers implementation problems when evaluating the sufficiency of the government's certification. Specifically, the FISC "has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired" and that "[s]ubstantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the communications of non-U.S. persons outside the United States." *See [Caption Redacted]*, 2011 WL 10945618, at *9 (internal quotation marks and citation omitted).

⁵² Depending on the type or severity of compliance incidents, the NSA also may promptly notify the relevant congressional intelligence committees of an individual compliance matter.

6. District Court Review of FISC Orders and Section 702 Collection

The FAA authorizes the use in a criminal prosecution of information obtained or derived from the acquisition of foreign intelligence information under Section 702, provided that advance authorization is obtained from the Attorney General and notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. Information acquired pursuant to Section 702 is “deemed to be” information acquired pursuant to Title I of FISA for, among other things, the purposes of the applicability of the statutory notice requirement and the suppression and discovery provisions of 50 U.S.C. § 1806. 50 U.S.C. § 1881e(a).

Under 50 U.S.C. § 1806(c), the government’s notice obligation applies only if (1) the government “intends to enter into evidence or otherwise use or disclose” (2) against an “aggrieved person” (3) in a “trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States” (4) any “information obtained or derived from” (5) an “electronic surveillance [or physical search] of that aggrieved person.” 50 U.S.C. § 1806(c); *see also* 50 U.S.C. § 1825(d).⁵³ When all five criteria are met, the government must notify the defense and the court presiding over the proceeding that the government intends to use or disclose such information. The “aggrieved” defendant may then challenge the use of that

⁵³ As noted above, an “aggrieved person” is defined as the target of electronic surveillance or “any other person whose communications or activities were subject to electronic surveillance,” 50 U.S.C. § 1801(k), as well as “a person whose premises, property, information, or material is the target of physical search” or “whose premises, property, information, or material was subject to physical search.” 50 U.S.C. § 1821(2). Contrary to the defendant’s contention (Doc. 48 at 27), however, FISA does not confer on an aggrieved person Fourth Amendment protection to which that person is not otherwise entitled.

information in district court on two grounds: (1) that the information was unlawfully acquired; or (2) that the acquisition was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e)-(f), 1881e(a).⁵⁴ In assessing the legality of the collection at issue, the district court, “shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted.” 50 U.S.C. §§ 1806(f), 1825(g). The Attorney General has filed such a declaration contemporaneously with this memorandum. See Sealed Exhibit 1.

On the filing of the Attorney General’s affidavit or declaration, the court “may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] *only* where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search].” 50 U.S.C. §§ 1806(f), 1825(g) (emphasis supplied). If the district court is able to make an accurate determination of the legality of the surveillance or search based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the court may not

⁵⁴ Separately, any electronic communications service provider the government directs to assist in Section 702 surveillance may challenge the lawfulness of that directive before the FISC. See 50 U.S.C. § 1881a(h)(4) and (6); see also *In re Directives*, 551 F.3d at 1004 (adjudicating Fourth Amendment challenge brought by electronic communications service provider to directive issued under the PAA, which was the predecessor to Section 702).

order disclosure of any of the FISA or Section 702 materials to the defense. *See* 50 U.S.C. §§ 1806(f), 1825(g); *see also Daoud*, 755 F.3d at 484. Although defendant did not seek disclosure of any of the FISA or Section 702 materials, it is nonetheless worth noting that federal courts, including the U.S. Court of Appeals for the Seventh Circuit, have repeatedly and consistently held that FISA anticipates that an *ex parte*, *in camera* determination is to be the rule. *Daoud*, 755 F.3d at 484 (“[u]nless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance, . . . there is no basis for concluding that disclosure is necessary”); *see also In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury* (“*In re Grand Jury Proceedings*”), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials). In fact, every court but one (whose decision was subsequently overturned by an appellate court)⁵⁵ that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera*, *ex parte* review. *See, e.g., United States v. Omar*, 786 F.3d 1104, 1110-11 (8th Cir. 2015); *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991) (“study of the materials leaves no doubt that substantial national security interests required the *in camera*, *ex parte* review, and that the district court properly conducted such a review”); *United States v.*

⁵⁵ The district court in *United States v. Daoud*, No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014), ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials. The government appealed the district court’s order to the Seventh Circuit, which overturned the district court’s decision to disclose, stating, “So clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so.” *Daoud*, 755 F.3d at 485.

El-Mezain, 664 F.3d 467, 566 (5th Cir. 2011) (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *United States v. Abu-Jihaad*, 630 F.3d 102, 129-30 (2d Cir. 2010).

IV. THE DEFENDANT'S CONSTITUTIONAL ARGUMENTS LACK MERIT

The defendant has moved for suppression of evidence derived from the acquisition of foreign intelligence information under Section 702 on the ground that Section 702 is unconstitutional. (Doc. 48 at 24-52) For the reasons stated below, the motion to suppress should be denied.

A. THE ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION UNDER SECTION 702 IS LAWFUL UNDER THE FOURTH AMENDMENT

For the reasons set forth below, the collection at issue in this case, pursuant to Section 702 and the applicable certification(s) and targeting and minimization procedures, was consistent with the Fourth Amendment. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" and that "no Warrants shall issue, but upon probable cause." "[A]lthough both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search," *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (citation omitted), "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665 (1989). The "touchstone" of a Fourth Amendment analysis "is always '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)).

The Section 702-authorized collection at issue in this case, which was conducted pursuant to court-approved procedures reasonably designed to target non-U.S. persons located outside the United States, was reasonable under the Fourth Amendment. As an initial matter, the Fourth Amendment generally does not apply to non-U.S. persons abroad. Further, the fact that collection targeting such persons also incidentally collects communications of U.S. persons or persons located in the United States does not trigger a warrant requirement or render the collection constitutionally unreasonable. Finally, surveillance conducted under Section 702 falls within the well-recognized “foreign intelligence exception” to the warrant requirement because (1) the government’s purpose—protecting against terrorist attacks and other external threats—extends “beyond routine law enforcement,” and (2) “insisting upon a warrant would materially interfere with the accomplishment of that purpose.” *In re Directives*, 551 F.3d at 1010-11.

Given the inapplicability of the warrant requirement, the challenged collection need, at most, only meet the Fourth Amendment’s general reasonableness standard. That standard is satisfied here. The government has interests of the utmost importance in obtaining foreign intelligence information under Section 702 to protect national security. In contrast, the privacy interests of persons located in the United States in international communications are significantly diminished when those

communications have been transmitted to or obtained from non-U.S. persons located outside the United States. Finally, the privacy interests of U.S. persons and persons located in the United States whose communications are incidentally collected are amply protected by stringent safeguards the government employs in implementing the collection. Those safeguards include: (1) certifications by Executive Branch officials concerning the permissible foreign intelligence purposes of the collection; (2) court-approved targeting procedures designed to ensure that only non-U.S. persons abroad are targeted; (3) court-approved minimization procedures to protect the privacy of U.S. persons (and, in certain limited circumstances, non-U.S. persons) located in the United States whose communications are incidentally acquired; (4) the requirement of a significant purpose to obtain foreign intelligence information; (5) extensive oversight within the Executive Branch, as well as by Congress and the FISC; and (6) a prior judicial finding that the targeting and minimization procedures are consistent with the Fourth Amendment.

In light of these and other safeguards, the FISC has repeatedly concluded that acquisition of foreign intelligence information under Section 702 and the applicable targeting and minimization procedures is constitutionally reasonable. A unanimous panel of the Ninth Circuit recently upheld the constitutionality of Section 702 in affirming the denial of a motion to suppress Section 702-derived evidence, and in doing so, rejected many of the same arguments that the defendant raises here. *See*

Mohamud II, 843 F.3d at 437-44.⁵⁶ And the district courts that have decided a motion to suppress Section 702-derived evidence on the merits have reached the same result. See *United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500 (E.D.N.Y. Mar. 8, 2016); *United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or. June 24, 2014) (“*Mohamud I*”), *aff’d*, *Mohamud II*, 843 F.2d 420; *United States v. Muhtorov*, No. 12-cr-00033-JLK (D. Colo. Nov. 19, 2015) (slip op.).⁵⁷ This Court should reach the same conclusion.

**1. There Is No Judicial Warrant Requirement
Applicable to Foreign Intelligence Collection Targeted
at Foreign Persons Abroad**

**a. The Fourth Amendment Generally Does Not Apply to
Non-U.S. Persons Abroad**

The Supreme Court has held that the Fourth Amendment does not “apply to activities of the United States directed against aliens in foreign territory.” *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990); see also *id.* at 271 (noting that only persons who “have come within the territory of the United States and developed substantial connections” to the country have Fourth Amendment rights). Based on the Fourth Amendment’s text, drafting history, and post-ratification history, *id.* at 265-67, as well as its own precedents, *id.* at 268-71, the Supreme Court concluded that the

⁵⁶ On March 16, 2017, the Ninth Circuit entered an order denying Mohamud’s petition for panel rehearing and rehearing en banc. Order, *United States v. Mohamud*, No. 14-30217 (9th Cir. Mar. 16, 2017). The order stated that the panel had voted to deny the petition for panel rehearing and that “no active judge ha[d] requested a vote on whether to rehear the matter en banc.” *Id.* at 1.

⁵⁷ [CLASSIFIED MATERIAL REDACTED]

Fourth Amendment was not intended “to restrain the actions of the Federal Government against aliens outside of the United States territory.” *Id.* at 266. “If there are to be restrictions on searches and seizures which occur incident to such American action,” the Court explained, “they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.” *Id.* at 275. Because the Fourth Amendment generally does not protect non-U.S. persons outside the United States, the government may lawfully subject them to surveillance without a warrant.

Intelligence collection under Section 702 targets non-U.S. persons located outside the United States. Accordingly, under *Verdugo*, the Fourth Amendment is generally inapplicable to persons who are targeted for collection in accordance with the requirements of the statute.⁵⁸ For that reason, to the extent the defendant attempts a facial challenge to Section 702 (*see, e.g.*, Doc. 48 at 5, 31, 46), the challenge fails, because the statute is constitutional in its application to persons unprotected by the Fourth Amendment. *See United States v. Salerno*, 481 U.S. 739, 745 (1987) (noting that, outside of the First Amendment context, a statute is facially invalid only if it is unconstitutional in all of its possible applications).⁵⁹

⁵⁸ The head of each element of the intelligence community must report annually to the FISC concerning, *inter alia*, how many persons the element targeted under Section 702 (based on the belief that the persons were located outside the United States) who were later determined to be located inside the United States. *See* 50 U.S.C. § 1881a(i)(3)(A)(iii).

⁵⁹ The Supreme Court recently held in a civil case that there is no categorical bar to facial challenges under the Fourth Amendment. *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2449 (2015) (permitting a civil litigant to bring a facial challenge to a statute authorizing warrantless searches without presenting case-specific facts to support the claim). Nevertheless, any facial challenge to Section 702 would fail in light of the statute’s “plainly legitimate sweep” in its application to communications of non-U.S. persons abroad who lack Fourth Amendment rights. *See, e.g., Washington v. Glucksberg*, 521 U.S. 702, 740 n.7 (1997) (Stevens, J., concurring) (noting that even “the most lenient standard that [the Supreme Court

b. The Incidental Collection of Communications of Persons Protected by the Fourth Amendment Pursuant to Intelligence Collection Lawfully Targeting Non-U.S. Persons Located Outside the United States Does Not Trigger a Warrant Requirement

The defendant was not targeted under Section 702.⁶⁰ Rather, his communications were incidentally collected through Section 702 acquisitions targeting one or more non-U.S. persons located outside the United States.⁶¹

Section 702 does not permit the intentional targeting of U.S. persons or persons located in the United States. To the extent that the government *incidentally* collects the communications of U.S. persons or persons in the United States who communicate

has] applied requires the challenger to establish that the invalid applications of a statute must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep") (citation and internal quotation marks omitted). Accordingly, this Court's review should be limited to the constitutionality of the statute as applied to the acquisition of the information challenged in this case. *See Mohamud II*, 843 F.3d at 438 n.21 ("We do not read *Patel* to permit courts, in a criminal prosecution, to suppress evidence based on a Fourth Amendment challenge to techniques not employed in a particular case.").

⁶⁰ Citing *Verdugo*, the defendant, a non-U.S. person, argues (Doc. 48 at 24-27) that he is entitled to Fourth Amendment protection because he has "substantial connections" to the United States. In *Verdugo*, the Supreme Court held that the Fourth Amendment had "no application" to a criminal defendant because, "[a]t the time of the search" of his residence in Mexico, he was "a citizen and resident of Mexico with no voluntary attachment to the United States." 494 U.S. at 274-75. The Court distinguished decisions establishing that "aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country," explaining that the defendant in *Verdugo*, by contrast, "had no previous significant voluntary connection with the United States." *Id.* at 271.

The government does not argue that the Fourth Amendment is inapplicable to the defendant with respect to the Section 702 collection through which his communications were incidentally acquired. The Court therefore need not address the defendant's "substantial connections" argument. Instead, the Court should hold that the challenged Section 702 acquisitions were reasonable, and thus lawful, under the Fourth Amendment, as demonstrated below.

⁶¹ [CLASSIFIED MATERIAL REDACTED]

with Section 702 foreign targets, such “incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.” *Mohamud II*, 843 F.3d at 439 (quoting *In re Directives*, 551 F.3d at 1015); see also *United States v. White*, 401 U.S. 745, 751-53 (1971) (holding that a conversation recorded with the consent of one participant did not violate another participant’s Fourth Amendment rights); *United States v. Kahn*, 415 U.S. 143, 156-57 (1974) (upholding interception of communications of a woman that were incidentally collected pursuant to a criminal wiretap order targeting her husband); *United States v. Figueroa*, 757 F.2d 466, 472-73 (2d Cir. 1985) (rejecting challenge to Title III on the ground that it allows interception of conversations of unknown third parties); *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) (upholding the constitutionality of warrantless surveillance for foreign intelligence purposes even though “conversations . . . of American citizens[] will be overheard”); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) (“[I]ncidental interception of a person’s conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.”).⁶²

Under these principles, incidentally capturing communications of a U.S. person or a person located in the United States during surveillance that lawfully targets non-

⁶² Contrary to the defendant’s contention (Doc. 48 at 44-45), not all incidental collection cases involve acquisitions based on warrants. *White* involved surveillance based on consent; *In re Directives* involved warrantless foreign intelligence surveillance pursuant to the PAA (which, as noted above, was the predecessor to Section 702); and *Bin Laden* involved a warrantless search conducted abroad. “[W]hen the 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.” *Mohamud II*, 843 F.3d at 440-41 (citation omitted).

U.S. persons abroad does not imply that a judicial warrant or other individualized court order is required for such surveillance to be reasonable under the Fourth Amendment. *See Bin Laden*, 126 F. Supp. 2d at 281 (noting that “the combination of *Verdugo-Urquidez* and the incidental interception cases” would permit surveillance that collects a U.S. person’s communications as an incident to warrantless surveillance targeting a non-U.S. person abroad, so long as the U.S. person is not a “known and contemplated” surveillance target). Thus, as the Ninth Circuit recently concluded, surveillance of non-U.S. persons outside the United States pursuant to Section 702, even without a warrant or probable cause, is not rendered unlawful if the surveillance incidentally captures the communications of non-targeted persons in the United States. *See Mohamud II*, 843 F.3d at 439 (“Consistent with *Verdugo-Urquidez* and our precedent, we hold that this particular type of non-upstream collection—where a search was not directed at a U.S. person’s communications, though some were incidentally swept up in it—does not require a warrant, because the search was targeted at a non-U.S. person with no Fourth Amendment right.”).

The defendant is incorrect in asserting (Doc. 48 at 44) that “the concept of ‘targeting’ as applied by the Ninth Circuit [in *Mohamud II*] is contrary to Fourth Amendment law because it focuses on the intelligence agency’s subjective state of mind.” There is nothing subjective about targeting under Section 702 or about applying the incidental collection principle to collection thereunder. As discussed above, collection under Section 702 is implemented on a facility-by-facility basis. A particular facility may be tasked for collection only after the government has

reasonably determined based on the totality of the circumstances that the user of that facility is a non-U.S. person who is located outside the United States and that the tasking is likely to result in the acquisition of foreign intelligence information. As a matter of objective fact, that user is the target of the Section 702 collection, just as the user of a facility specified in a traditional FISA order or the subject of law enforcement intercept under Title III of the Wiretap Act (“Title III wiretap”) may be described as the target of those forms of collection. The defendant does not dispute that incidental collection is lawful in the context of electronic surveillance pursuant to traditional FISA orders or Title III wiretaps. The incidental collection principle applies precisely the same way in the context of Section 702.⁶³

The defendant also contends (Doc. 48 at 40-41) that incidentally collecting U.S. persons’ communications under Section 702 is unconstitutional because the government expects that some foreign targets will communicate with U.S. persons, and minimization procedures permit the government in certain circumstances to retain those communications. Once again, however, the same is true of traditional FISA electronic surveillance and Title III wiretaps. Under those authorities, the government also incidentally collects third party communications, and minimization procedures

⁶³ Citing *Bin Laden*, 126 F. Supp. 2d at 281, the defendant also asserts (Doc. 48 at 45) that the Ninth Circuit’s “‘targeting’ and ‘incidental overhear’ rationale [in *Mohamud II*] permit[s] the government to exploit a gap in the law, which has previously been rejected.” That assertion is incorrect. In *Bin Laden*, the court concluded that one of the defendants could not be considered an “‘incidental’ interceptee” with respect to collection directed at his own home and cellular telephones because “he was not an unanticipated user of those telephones and because he was believed to be a participant in the activities being investigated.” *Id.* The court agreed, however, that the incidental collection principle “would permit the surveillance if the Government had not been aware of [the defendant’s] identity or of his complicity in the enterprise.” *Id.*

permit the government to retain those communications in certain circumstances. Moreover, the fact that one purpose of Section 702 surveillance may be to discover whether the foreign targets are in contact with individuals in the United States does not mean that collection of such communications requires a separate warrant or is constitutionally unreasonable. *Mohamud II*, 843 F.3d at 440 (“The fact that the government knew some U.S. persons’ communications would be swept up during foreign intelligence gathering does not make such collection any more unlawful in this context than in the Title III or traditional FISA context.”); *see also United States v. McKinnon*, 721 F.2d 19, 22-23 (1st Cir. 1983) (“While an interception that is unanticipated is *a fortiori* incidental, the converse is not true; something does not have to be unanticipated in order to be incidental.”).

The defendant suggests (*see* Doc. 48 at 40) that Section 702 incidentally collects more U.S. person communications compared to traditional FISA electronic surveillance or Title III wiretaps, and that an exception to the incidental collection principle is therefore necessary. The defendant cites no authority suggesting that the lawfulness of the incidental collection depends on how extensively the government uses the particular surveillance authority at issue. Indeed, other courts have correctly rejected this claim. *See, e.g., Mohamud II*, 843 F.3d at 440. Moreover, insofar as the defendant suggests (*see, e.g.,* Doc. 48 at 40) that traditional FISA surveillance is less likely than Section 702 surveillance to result in the incidental collection of U.S. person communications, he is incorrect. Traditional FISA electronic surveillance, which unlike Section 702, can be used to target U.S. persons and persons in the United

States, is likely to capture a significantly larger concentration of non-targeted U.S. persons' communications than Section 702, which targets foreign communications. *See [Caption Redacted]*, 2011 WL 10945618, at *7. Incidentally collecting non-targeted third party communications under Section 702 is reasonable, just as it is under traditional FISA, because the surveillance is lawful as to the target, and no separate warrant is required as to those third parties.

Finally, the application of a warrant requirement to incidental collection of communications of persons located in the United States during surveillance targeting non-U.S. persons abroad for foreign intelligence purposes would be inconsistent with decades of foreign-intelligence collection practice. *See In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 169 (2d Cir. 2008) (holding that the warrant requirement does not apply to searches or surveillance of U.S. citizens that occur outside the United States because the original purpose of the Fourth Amendment "was to restrict searches and seizures which might be conducted by the United States in domestic matters"); *United States v. Barona*, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) (foreign searches have "neither been historically subject to the warrant procedure, nor could they be as a practical matter"); *United States v. Stokes*, 726 F.3d 880, 893 (7th Cir. 2013) (rejecting warrant requirement for extraterritorial searches targeting U.S. persons and holding such searches "are subject only to the Fourth Amendment's requirement of reasonableness").⁶⁴

⁶⁴ The defendant cites no authorities indicating that foreign intelligence collection targeting non-U.S. persons outside the United States requires a warrant.

Such a requirement would also be impracticable. Before initiating surveillance of a foreign target, the government cannot know the identities of all those with whom the target will communicate in the future, and there will generally be at least some possibility that the target will communicate with a U.S. person. *See Bin Laden*, 126 F. Supp. 2d at 280 (“[T]he government is often not in a position of omniscience regarding who or what a particular surveillance will record.”). Thus, the imposition of a warrant requirement for any incidental interception of communications of persons located in the United States would effectively require a warrant for *all* foreign intelligence collection, even though the foreign targets lack Fourth Amendment rights and their communications often only involve other foreigners. Such a rule would unduly restrict the government’s intelligence collection against foreign targets and degrade its ability to protect against foreign threats. *See Warrantless Surveillance and The Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans’ Privacy Rights (Part II)*, *Hearing Before the H. Judiciary Comm.*, 110th Cong., 8 (2007) (statement of Rep. Forbes) (“To require a court order for every instance in which a foreign target communicates with someone inside the United States is to require a court order for every foreign target, and requiring this would reverse 30 years of established intelligence gathering The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.”).

c. The Location of the Search Does Not Trigger a Warrant Requirement

Verdugo involved a physical search that was conducted overseas, while collection under Section 702 takes place within the United States. The defendant is incorrect in asserting (*see* Doc. 48 at 24-26) that the location of the collection is constitutionally significant in this case. In the context of electronic communications, the fact that the communications of a non-U.S. person outside the United States may be collected from within the United States is insufficient to bring that person within the protection of the Fourth Amendment under *Verdugo*. As the Ninth Circuit recently explained, “what matters here is the location of the *target*,’ and not where the government literally obtained the electronic data.” *Mohamud II*, 843 F.3d at 439 (quoting *Hasbajrami*, 2016 WL 1029500, at *9 n.15) (emphasis in original). Otherwise, any foreign person abroad seeking to evade U.S. government surveillance, including an ISIL or al Qaeda terrorist, could claim the protections of the Fourth Amendment merely due to the fortuity that in some cases their communications might be collected from inside the United States rather than abroad. That result would be plainly contrary to the Supreme Court’s statements in *Verdugo* that the Fourth Amendment was not originally intended to protect “aliens outside of the United States territory.” *Verdugo*, 494 U.S. at 266-67.

Moreover, contrary to the defendant’s contention (Doc. 48 at 24-26), when the U.S. government collects the communications of a non-U.S. person located abroad, whether the collection takes place in the United States or abroad makes no difference to the person’s privacy interests and should not affect the constitutional analysis. When it comes to the content of communications, “the Fourth Amendment protects

people, not places.” *United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir. 1983) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). Accordingly, there is no “constitutional distinction which depends upon the location of the recording apparatus.” *Id.*

2. The Foreign Intelligence Exception Applies

Even assuming *arguendo* that the incidental collection of communications of persons located in the United States under Section 702 is subject to the same constitutional scrutiny as foreign intelligence collection targeting such persons, the Fourth Amendment does not require a warrant here because such surveillance falls within the well-recognized foreign intelligence exception to the warrant requirement.

a. The “Special Needs” Doctrine

The touchstone of the Fourth Amendment is reasonableness, which is assessed by balancing the degree to which a search is needed to promote legitimate governmental interests against the search’s intrusion on a person’s privacy interests. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001). “Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant.” *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995). But that procedure is by no means inflexibly required. *See Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (The Fourth Amendment “imposes no irreducible requirement” of individualized suspicion.).

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable," *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotation marks omitted), such as where the governmental need is especially compelling or especially likely to be frustrated by a warrant requirement, where expectations of privacy are diminished, and where alternative safeguards restrain the government within reasonable limits. *See King*, 133 S. Ct. at 1969 (upholding warrantless collection of DNA sample from felony arrestee); *see also, e.g., Griffin*, 483 U.S. at 873-74 (upholding warrantless search of probationer's home); *Vernonia Sch. Dist.*, 515 U.S. at 653 (upholding warrantless drug testing of student-athletes by public school district); *Samson v. California*, 547 U.S. 843, 847 (2006) (upholding suspicionless searches of parolees). In evaluating whether the "special needs" doctrine applies, the Supreme Court has distinguished between searches designed to uncover evidence "of ordinary criminal wrongdoing" and those motivated "at [a] programmatic level" by other governmental objectives. *City of Indianapolis v. Edmond*, 531 U.S. 32, 37-40, 48 (2000) (reviewing cases).

The "special needs" doctrine applies where special government interests beyond the normal need for law enforcement make the warrant and probable-cause requirement impracticable, and in such cases the court "employ[s] a balancing test that weigh[s] the intrusion on the individual's interest in privacy against the 'special needs' that supported the program." *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001). Accordingly, the Supreme Court has permitted, *inter alia*, warrantless stops of

motorists at roadblocks for the purpose of securing borders, *see United States v. Martinez-Fuerte*, 428 U.S. 543, 543 (1976), warrantless searches of the homes of probationers to ensure compliance with probation conditions, *see Griffin*, 483 U.S. at 872, and warrantless searches of public school students to enforce school rules, *see T.L.O.*, 469 U.S. at 340.

b. The Foreign Intelligence Exception

Several courts of appeals—including the FISA Court of Review—have held, by analogy to the “special needs” doctrine, that the government’s “special need” for foreign intelligence information justifies an exception to the warrant requirement. *See, e.g., United States v. Duka*, 671 F.3d 329, 341 (3d Cir. 2011) (“[C]ourts [that have considered the question] almost uniformly have concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of ‘foreign intelligence exception’ to the Fourth Amendment’s warrant requirement.”); *In re Directives*, 551 F.3d at 1010-11 (recognizing “a foreign intelligence exception” to the warrant requirement); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) (“[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.”); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980) (upholding warrantless foreign intelligence surveillance authorized by the Attorney General); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) (“Foreign security wiretaps are a recognized exception to the general warrant requirement.”); *Butenko*, 494 F.2d at 605; *United States v. Brown*, 484

F.2d 418, 426 (5th Cir. 1973).⁶⁵ *But see Zweibon v. Mitchell*, 516 F.2d 594, 618-20 (D.C. Cir. 1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation).⁶⁶ Foreign intelligence collection justifies an exception because the “programmatically 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.

Contrary to these decisions, the defendant contends (Doc. 48 at 34) that the foreign intelligence exception is narrow and applies only when the search is minimally intrusive and executive discretion is strictly confined. There is no such limitation on the doctrine. *Cf. MacWade v. Kelly*, 460 F.3d 260, 269 (2d Cir. 2006) (noting, in upholding warrantless subway searches to prevent terrorist attacks, that “[t]he Supreme Court never has implied—much less actually held—that a reduced privacy expectation is a *sine qua non* of special needs analysis”). While considerations of intrusiveness and executive discretion may be relevant to the reasonableness of a government program designed to serve a special need, neither factor is decisive regarding whether the doctrine applies at the threshold as an exception to the warrant

⁶⁵ Except for *In re Directives*, these cases involved collection of foreign intelligence information from persons inside the United States. Their reasoning applies *a fortiori* to the Section 702 acquisitions in this case, which targeted non-United States person(s) reasonably believed to be outside the United States.

⁶⁶ The plurality in *Zweibon* specifically noted that the surveillance at issue targeted a domestic organization and suggested that its conclusion might be different if a foreign power were targeted. *See* 516 F.2d at 651.

clause. *See id.* at 268-69 (addressing such factors under the general reasonableness test, separately from the threshold question whether the searches served a governmental purpose distinct from ordinary law enforcement).

The defendant's reliance (*see* Doc. 48 at 28-30, 35) on *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), is misplaced. The Court in *Keith* expressly reserved the issue of a warrant requirement for foreign intelligence collection. *See id.* at 308-09. Moreover, *Keith* "implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible." *Clapper*, 133 S. Ct. at 1143; *see also In re Sealed Case*, 310 F.3d at 738. The same rationale "applies *a fortiori* to foreign threats," a fact that Congress necessarily recognized in enacting FISA. *In re Sealed Case*, 310 F.3d at 738; *see also Truong*, 629 F.2d at 913 ("For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities.").

In addition, unlike Section 702 intelligence collection, the surveillance in *Keith* was conducted not only without a warrant but without any judicial or congressional oversight of any kind. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-37 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum."). The courts that have addressed the issue whether foreign intelligence collection is subject to a warrant requirement have expressly distinguished *Keith* in holding that it is not. *See In re*

Directives, 551 F.3d at 1010; *In re Sealed Case*, 310 F.3d at 744; *Truong*, 629 F.2d at 913; *Butenko*, 494 F.2d at 602 n.32; *Brown*, 484 F.2d at 425.

In sum, courts have generally recognized, by analogy to the “special needs” doctrine, that a foreign intelligence exception to the warrant requirement exists. As the FISC has held, and for the reasons set forth below, that exception applies to acquisitions under Section 702. *See [Caption Redacted]*, 2011 WL 10945618, at *24 (“The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the ‘foreign intelligence exception’ to the warrant requirement of the Fourth Amendment.”); *see also Mohamud I*, 2014 WL 2866749, at *18 (holding that “the foreign intelligence exception applies” to Section 702 collection and therefore “no warrant is required”).

c. The Government’s Purpose in Section 702 Collection Goes Beyond Ordinary Crime Control

The government’s programmatic purpose in obtaining the information pursuant to Section 702 goes well beyond routine law enforcement. *See In re Sealed Case*, 310 F.3d at 746 (holding that the government’s “programmatic purpose” in obtaining foreign intelligence information is “to protect the nation against terrorists and espionage threats directed by foreign powers”—“a special need” that fundamentally differs from “ordinary crime control”); *see also Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (upholding warrantless searches of ferry passengers because “[p]reventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs and indeed go well beyond them”). Acquisitions under Section 702 must be conducted with a “significant purpose” to “obtain foreign intelligence

information.” 50 U.S.C. § 1881a(g)(2)(A)(v). As the FISA Court of Review found in the context of Section 702’s predecessor statute, the “stated purpose” of the collection “centers on garnering foreign intelligence,” and “[t]here is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes.” *In re Directives*, 551 F.3d at 1011. The same is true of collection authorized under Section 702 in this case.⁶⁷ *See Mohamud I*, 2014 WL 2866749, at *18.

For that reason, the defendant’s reliance (see Doc. 48 at 30, 32, 46) on *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), is misplaced. There, the Sixth Circuit held that “[t]he government may not compel a commercial [Internet Service Provider] to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause.” *Id.* at 288. But *Warshak* involved the government’s acquisition of a subscriber’s e-mail communications in the course of a criminal investigation. *Warshak* did not address the acquisition of electronic communications for foreign intelligence purposes, and the decision has no bearing on the applicability of the foreign intelligence exception to the warrant requirement. Accordingly, even assuming *arguendo* that the defendant had a reasonable expectation of privacy in this

⁶⁷ *See* Part III.C.4.a., *supra*. As the FISC found when it first ruled on the constitutionality of a Section 702 certification, the targeting procedures ensure that collection under Section 702 is undertaken for foreign intelligence purposes by requiring targets to be “assessed by NSA to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power authorized for acquisition under the Certification.” *See* Mem. Op. at 35, *In re DNI/AG Certification*, No. 702(i)-08-01 (FISA Ct. Sept. 4, 2008) (“*Sept. 2008 FISC Op.*”), available at <https://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf>. *See also Duka*, 671 F.3d at 343-45 (surveillance based on the “significant purpose” test is reasonable under the Fourth Amendment).

case, see Part IV.A.3.b., *infra*, *Warshak* does not undermine the lawfulness of the acquisition of his communication(s) under Section 702.

d. A Warrant or Probable Cause Requirement Would Be Impracticable

As the FISA Court of Review found with respect to Section 702's predecessor statute, "there is a high degree of probability that 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. "[A]ttempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy," and, therefore, "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *Truong*, 629 F.2d at 913.⁶⁸ Changes in technology and the manner of collecting foreign intelligence information make timing concerns even more acute; requiring a warrant as to targets or third-party communicants would undermine the vital national security purposes of the collection.

When the government has reason to believe that a non-U.S. person overseas is connected to international terrorist activities, but the government lacks sufficient evidence to establish probable cause that the target is an agent of a foreign power, a

⁶⁸ In connection with its review of the first Section 702 certification, the FISC found that the same considerations apply to Section 702 collection, which "similarly involves targets who are attempting to conceal their communications, thereby presenting the same concerns that weigh against requiring the government to obtain a warrant." *Sept. 2008 FISC Op.* at 36.

warrant requirement could prevent the government from obtaining significant information. Even when the government succeeds in eventually gathering enough information to establish probable cause under FISA, the need to develop such information and to obtain FISC approval could result in delays that would hinder the government's ability to monitor fast-moving threats. *See In re Directives*, 551 F.3d at 1011-12 (“[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government’s ability to collect information in a timely manner”); PCLOB Report at 104-06 (recognizing value in the “flexibility” that Section 702 provides by “allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision”); *cf. Verdugo*, 494 U.S. at 273-74 (“Application of the Fourth Amendment” to aliens abroad could “significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest.”).

In short, a warrant requirement would significantly undermine the government's ability to obtain foreign intelligence information vital to the nation's security. *See Bin Laden*, 126 F. Supp. 2d at 273 (concluding that “the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden” on the government’s ability to obtain foreign intelligence information). That would be a particularly unnecessary result because Section 702 collection does not target U.S. persons or persons located in the United States, *see* 50 U.S.C. § 1881a(b), and the law contains robust safeguards that protect the interests of such persons

whose communications might be incidentally collected. *See Abu-Jihaad*, 630 F.3d at 121-22 (“[T]he Constitution’s warrant requirement is flexible, so that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations at issue.”) (internal quotation marks and citation omitted).⁶⁹

e. A Warrant Requirement Would Inappropriately Interfere with Executive Branch Discretion in the Collection of Foreign Intelligence

The Fourth Amendment’s warrant requirement is based in part on the interest in “interpos[ing] a judicial officer between the zealous police officer ferreting out crime and the subject of the search.” *In re Terrorist Bombings*, 552 F.3d at 170 n.7. But that concern is considerably diminished in this context because of “the acknowledged wide discretion afforded the executive branch in foreign affairs.” *Id.*; *see Truong*, 629 F.2d at 914 (“[T]he executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.”). For that reason, the Fourth Amendment does not require that courts interpose themselves in the Executive Branch’s collection of foreign intelligence beyond the procedures provided for by Congress.

⁶⁹ A number of courts have recognized the continuing validity of the rationale for the foreign intelligence exception even after the enactment of FISA created a regime in which the government could obtain a court order to conduct foreign intelligence surveillance in certain circumstances. *See, e.g., In re Directives*, 551 F.3d at 1010-11; *In re Sealed Case*, 310 F.3d at 742; *Duka*, 671 F.3d at 341; *[Caption Redacted]*, 2011 WL 10945618, at *24; *Mohamud I*, 2014 WL 2866749, at *18.

f. Section 702 Falls Within the Scope of the Foreign Intelligence Exception

The defendant contends (Doc. 48 at 34) that the foreign intelligence exception is limited to circumstances where: (1) the surveillance was directed at a specific foreign agent or foreign power; (2) the *primary* purpose was to gather foreign intelligence information; and (3) the surveillance was personally approved by the President or Attorney General. This argument should be rejected.

The specific foreign-agent-or-power limitation was recognized in *Truong*, which involved unilateral Executive Branch surveillance directed at a person within the United States. *See* 629 F.2d at 911-13. However, nothing in *Truong* or the other decisions cited by the defendant suggests that foreign intelligence surveillance directed at non-U.S. persons outside the United States, as authorized by Congress and conducted pursuant to targeting and minimization procedures approved by the FISC, must be directed only at a specific foreign agent or foreign power. And, for the reasons explained above, such a requirement would seriously undermine the government's ability to obtain foreign intelligence information in this context and, in any event, would be unnecessary since the targets of the surveillance are persons unprotected by the Fourth Amendment.

The defendant's second argument invokes the purported "primary purpose" requirement that has been repeatedly rejected by Congress and the courts. *See In re Directives*, 551 F.3d at 1011; *In re Sealed Case*, 310 F.3d at 742-45; *Abu-Jihaad*, 630 F.3d at 121; *Duka*, 671 F.3d at 343-45. As the FISA Court of Review has explained, the "primary purpose" language adopted in *Truong* "drew an unstable, unrealistic, and

confusing line between foreign intelligence purposes and criminal investigation purposes.” *In re Directives*, 551 F.3d at 1011 (internal quotation marks omitted).

Because “surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose,” such as “apprehension of terrorism suspects,” *id.*, attempting to discern whether criminal-law purposes are primary or secondary to intelligence purposes can be an artificial exercise. *See In re Sealed Case*, 310 F.3d at 743.

Accordingly, “the more appropriate consideration is the programmatic purpose of the surveillances and whether – as in the special needs cases – that programmatic purpose involves some legitimate objective beyond ordinary crime control.” *In re Directives*, 551 F.3d at 1011; *see also In re Sealed Case*, 310 F.3d at 745-46. In *In re Sealed Case*, the FISA Court of Review construed the “significant purpose” requirement to preclude the government from using FISA as a “device to investigate wholly unrelated ordinary crimes.” *Id.* at 735-36. Congress used the same term in Section 702’s predecessor statute, and Section 702 should be presumed to have incorporated this construction. *See Cannon v. Univ. of Chicago*, 441 U.S. 677, 696-99 (1979). So construed, the “significant purpose” standard is sufficient for purposes of the “special needs” doctrine and the “foreign intelligence” exception. *See Edmond*, 531 U.S. at 40-42 (noting that the doctrine turns on whether the programmatic purpose of a search goes beyond the investigation of “ordinary criminal wrongdoing”); *In re Directives*, 551 F.3d at 1011 (upholding directives under Section 702’s predecessor statute because “[t]heir stated purpose centers on garnering foreign intelligence” and “[t]here is no indication that the collections of information are primarily related to ordinary criminal-law enforcement

purposes”); *Mohamud I*, 2014 WL 2866749, at *18 (“There is no reasonable argument [that] the government’s need for the acquisitions is merely routine law enforcement.”).

As for the third purported limitation the defendant puts forward, it is true that the Attorney General does not personally approve each individual acquisition under Section 702. However, the Attorney General and the DNI play a significant role in establishing and authorizing the certification and procedures that govern the acquisition. *See* 50 U.S.C. § 1881a(a) (collection under Section 702 must be jointly authorized by the Attorney General and the DNI). In addition, unlike the unilateral executive branch surveillance in *Truong*, Section 702 collection is governed by stringent, court-approved procedural safeguards and extensive oversight by the FISC and by Congress. Those requirements provide sufficient authorization and oversight, by all three branches of government, for purposes of the foreign intelligence exception.

3. Foreign Intelligence Collection Pursuant to Section 702 Is Reasonable

In circumstances where a warrant and probable cause are not required, searches and seizures are generally subject to the Fourth Amendment’s “traditional standards of reasonableness.” *King*, 133 S. Ct. at 1970 (internal quotation marks omitted); *see id.* (“To say that no warrant is required is merely to acknowledge that rather than employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable.”) (internal quotation marks and citation omitted). In assessing the constitutional reasonableness of a government search, the court must weigh “the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an

individual's privacy." *Id.* (internal quotation marks omitted). The court determines what is reasonable, and what safeguards may be necessary in a particular context, by balancing the interests at stake in light of "the totality of the circumstances." *Samson*, 547 U.S. at 848 (internal quotation marks omitted); *see also Von Raab*, 489 U.S. at 665, 668 (recognizing that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance" and that "the traditional probable-cause standard may be unhelpful" when the government "seeks to *prevent*" dangers to public safety); *In re Directives*, 551 F.3d at 1012 (reviewing collection pursuant to Section 702's predecessor statute under the general reasonableness test).

Under the general reasonableness balancing test, searches without a warrant or individualized finding of probable cause are particularly likely to be found reasonable when the governmental need is especially great or especially likely to be frustrated by a warrant requirement, when the search involves modest intrusions on the individual's privacy, and when alternative safeguards restrain the government within reasonable limits. *See, e.g., Illinois v. McArthur*, 531 U.S. 326, 330-31 (2001) ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."); *King*, 133 S. Ct. at 1969 (warrantless search may be reasonable where "the public interest is such that neither a warrant nor probable cause is required" or where "an individual is already on notice . . .

that some reasonable [government] intrusion on his privacy is to be expected”) (citation and internal quotation marks omitted).

The Supreme Court recently engaged in this kind of balancing in *King*, which involved warrantless searches of arrestees to obtain DNA samples. 133 S. Ct. at 1968-69. The Court examined the totality of the circumstances, weighed the various interests at stake, and concluded, in light of the government’s “substantial . . . interest” in the “identification of arrestees,” the diminished expectations of privacy of an individual taken into police custody, and statutory protections that limited the purposes for which the DNA evidence could be collected and stored, that the balance favored the government. *Id.* at 1977-80; *see also Samson*, 547 U.S. at 848-57 (applying reasonableness balance in upholding warrantless, suspicionless search of the person of a parolee).

In *In re Directives*, the FISA Court of Review applied the general reasonableness test in considering the constitutional reasonableness of Section 702’s predecessor statute, the PAA, in the context of an as-applied challenge brought by a private party that had been directed by the government to assist in effectuating surveillance under the statute. 551 F.3d at 1012-15.⁷⁰ In balancing the respective interests, the FISA

⁷⁰ The PAA was not identical to, and in certain respects was broader than, Section 702. Notably, the PAA authorized surveillance concerning “persons reasonably believed to be outside the United States” without distinguishing between U.S. and non-U.S. persons, *In re Directives*, 551 F.3d at 1007, while Section 702 authorizes only surveillance targeting non-U.S. persons outside the United States. In addition, the petitioner in *In re Directives* limited its claims to alleged injuries to U.S. persons. Accordingly, the analysis in *In re Directives* addresses certain issues specific to foreign intelligence surveillance targeted at U.S. persons abroad, including a requirement that surveillance targeting U.S. persons be based on a finding by the Attorney General of probable cause to believe that the U.S. person was a foreign power or agent of a foreign power, that are not applicable here.

Court of Review recognized that the government's interest in national security was of such a "high[] order of magnitude" that it would justify significant intrusions on individual privacy. *Id.* at 1012. The FISA Court of Review noted further that the PAA, the certification(s), and the directives contained a "matrix of safeguards," *id.* at 1013, including "effective minimization procedures" that were "almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions," *id.* at 1015, as well as "targeting procedures" that included "provisions designed to prevent errors" and provided for Executive Branch and congressional oversight of "compliance with th[e] [targeting] procedures," *id.* The FISA Court of Review concluded, based on the panoply of safeguards in the statutory provisions and implementing procedures, that "the surveillances at issue satisfy the Fourth Amendment's reasonableness requirement." *Id.* at 1016.⁷¹

The FAA provisions, certification(s), and procedures at issue in this case, with respect to collection targeting non-U.S. persons overseas, are as protective as, and in some respects significantly more robust than, the comparable procedures that the FISA Court of Review found constitutional.⁷² In addition, Section 702 goes beyond the PAA by requiring a prior finding by the FISC that the targeting and minimization procedures are reasonable under the Fourth Amendment. 50 U.S.C. § 1881a(i).

⁷¹ *In re Directives* was not litigated *ex parte*. The FISA Court of Review considered briefing and oral argument from both the government and the communications provider that challenged the directives. See 551 F.3d at 1008.

⁷² See *Sept. 2008 FISC Op.* at 38-39 & n.46 (recognizing that the targeting procedures at issue in *In re Directives* and the targeting procedures pursuant to the Section 702 certification included "substantively identical" factors for determining whether the person to be targeted "possesses and/or is likely to communicate foreign intelligence information") (citation and internal quotation marks omitted).

Section 702, unlike the PAA, also expressly prohibits “reverse targeting” of U.S. persons or the targeting of persons “known at the time of acquisition to be located in the United States.” 50 U.S.C. § 1881a(b)(1) and (2). Section 702 thus stands on an even firmer constitutional foundation than the PAA, and the FISA Court of Review’s analysis upholding the latter applies also to the former.

In addition, the FISC has repeatedly reviewed the targeting and minimization procedures controlling the government’s acquisition of foreign intelligence information under Section 702 and held that acquisitions pursuant to those procedures satisfy the Fourth Amendment reasonableness standard. *See [Caption Redacted]*, 2011 WL 10945618, at *6 (“The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of [Section 702] and with the Fourth Amendment.”); *see also, e.g.*, Mem. Op. and Order at 12, *[Caption Redacted]* (FISA Ct. Nov. 6, 2015) (“*Nov. 2015 FISC Op.*”).⁷³ The other courts to have considered the question, including the Ninth Circuit, have likewise found that, in light of the statutory protections governing Section 702 collection, the government’s compelling interest in protecting national security outweighs the intrusion of Section 702 surveillance on an individual’s privacy and therefore the Section 702 acquisitions at issue in those cases were “reasonable under the Fourth Amendment.” *Mohamud II*, 843 F.3d at 441; *see also Mohamud I*, 2014 WL 2866749, at *27; *Hasbajrami*, 2016 WL

⁷³ Available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

1029500, at *10-13; *Muhtorov*, slip op. at 27. There is no reason for a different outcome here.

**a. Acquisitions Under Section 702 Advance the
Government's Compelling Interest in Obtaining Foreign
Intelligence Information to Protect National Security**

The government's national security interest in conducting acquisitions pursuant to Section 702 "is of the highest order of magnitude." *See In re Directives*, 551 F.3d at 1012; *see also In re Certified Question of Law*, --- F.3d ---, 2016 WL 8923919, at *15 (FISA Ct. Rev. Apr. 14, 2016) ("[T]he Government's investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process."); *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.") (citation omitted). The terrorist threat the United States is facing today "may well involve the most serious threat our country faces." *In re Sealed Case*, 310 F.3d at 746; *see also Mohamud II*, 843 F.3d at 441 ("[T]he Government's interest in combating terrorism is an urgent objective of the highest order.") (quoting *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010)); *Duka*, 671 F.3d at 340 ("The government's interests in security and intelligence are entitled to particular deference."). Courts have recognized that the government's compelling interest in collecting foreign intelligence information to protect the nation against terrorist groups and other foreign threats may outweigh individual privacy interests. *See, e.g., In re Terrorist Bombings*, 552 F.3d at 172-76 (upholding search and surveillance targeting

U.S. person abroad because the intrusion on the individual's privacy was outweighed by the government's need to monitor the activities of al Qaeda).

The collection authorized by Section 702 is crucial to the government's efforts against terrorism and other threats both to the United States and its interests abroad. See National Security Agency, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* (Aug. 9, 2013), available at <https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml> ("[C]ollection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."). As the Senate Select Committee on Intelligence found in recommending reauthorization of the FAA in 2012, "the authorities provided under the [FAA] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets." S. Rep. No. 112-174, at 2 (2012); see also *id.* at 17 (Appendix) (DOJ paper noting that Section 702, in addition to "provid[ing] information about the plans and identities of terrorists" also enables the government to collect "information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States"). The Committee noted further that "failure to reauthorize section 702" would "result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities." *Id.*; see also H.R. Rep. No. 112-645, pt. 2, at 3 (2012) ("The importance of the collection of foreign intelligence under the [FAA] . . . cannot be underscored enough. . . . The information collected

under this authority is often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world.”).

The PCLOB found that Section 702 has “proven valuable in a number of ways to the government’s efforts to combat terrorism.” PCLOB Report at 107. The PCLOB noted that “over a quarter of the NSA’s reports concerning international terrorism include information based in whole or in part on Section 702 collection,” and that Section 702 collection is a uniquely valuable tool in enabling the government to discover and to monitor terrorist networks despite the terrorists’ efforts to conceal their activities and communications. *Id.* at 104-08. The PCLOB reviewed numerous specific instances in which Section 702 collection contributed to a counterterrorism investigation and found that information obtained through Section 702 has played a key role in “the discovery of previously unknown terrorist plots” and has “directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries.” *Id.* at 108-09. Finally, the PCLOB noted that Section 702 has also proven “highly valuable” in serving foreign intelligence purposes other than preventing terrorism, including countering the efforts of proliferators of weapons of mass destruction. *Id.* at 110. Thus, as the Executive Branch, Congress, the FISC, and the PCLOB have all recognized, the government has an extraordinarily compelling interest in conducting the collection authorized by Section 702.

b. U.S. Persons and Persons in the United States Have, at Most, Limited Expectations of Privacy in Electronic Communications With Non-U.S. Persons Outside the United States

The other side of the Fourth Amendment reasonableness balance is the degree to which the search “intrudes upon an individual’s privacy.” *Knights*, 534 U.S. at 118-19 (citation omitted). When the search takes place in circumstances in which the individual’s expectations of privacy are limited, the diminished character of the privacy interest must be taken into account in the court’s assessment of reasonableness. In the context of incidental collection, the privacy interests of U.S. persons or persons located in the United States in communications are significantly diminished when those communications have been transmitted to or obtained from non-U.S. persons located abroad.

As an initial matter, such persons have no cognizable Fourth Amendment interest in the communications facilities used by the foreign targets of the collection. *See Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (Fourth Amendment rights are personal and may not be asserted vicariously). Moreover, the Supreme Court has long held that when one person voluntarily discloses information to another, the first person loses any cognizable interest under the Fourth Amendment in what the second person does with the information. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Couch v. United States*, 409 U.S. 322, 335 (1973); *White*, 401 U.S. at 752 (plurality opinion); *Hoffa v. United States*, 385 U.S. 293, 302-03 (1966). For Fourth Amendment purposes, the same principle applies whether the recipient intentionally makes the information public or stores it in a place subject to a government search. Thus, once a non-U.S.

person located outside the United States receives information, the sender generally loses any cognizable Fourth Amendment rights with respect to that information. That is true even if the sender is a person protected by the Fourth Amendment, because he assumes the risk that the foreign recipient will give the information to others, leave the information freely accessible to others, or that the U.S. government (or a foreign government) will obtain the information.⁷⁴

This rule applies to physical mail, even within the United States. Although the Fourth Amendment protects sealed letters in transit, once a letter is sent to someone, “the sender’s expectation of privacy ordinarily terminates upon delivery.” *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995). The same rule applies to e-mail users, who lack “a legitimate expectation of privacy in an email that had already reached its recipient.” *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001); *see also United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (An “expectation of privacy may be diminished” for “transmissions over the Internet or email[s] that have already arrived at the recipient.”) (citation and internal quotation marks omitted); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (noting that a sender of e-mail, like a letter-writer, would lose an objective expectation of privacy in e-mail that the recipient had received).⁷⁵

⁷⁴ The “recipient” in this context refers to the ultimate recipient, not (for example) an internet service provider. *See Warshak*, 631 F.3d at 282-88.

⁷⁵ Moreover, any expectation of privacy of the defendant in his electronic communications with a non-U.S. person overseas is further diminished by the prospect that his foreign correspondence could be a target for surveillance by foreign governments or private entities, whose activities are not governed by the U.S. Constitution or federal law, or by the U.S. government, pursuant to various authorities applicable to foreign intelligence surveillance

Under these principles, the defendant's rights in communication(s) acquired by targeting the account(s) of other(s) were significantly diminished, if not lost altogether, at the time of collection. *See Mohamud II*, 843 F.3d at 442 (noting that defendant's expectation of privacy had been "diminished" in e-mail incidentally collected under Section 702 that defendant had sent to a third party).⁷⁶

c. Stringent Safeguards and Procedures Protect the Privacy Interests of U.S. Persons and Others Whose Communications Are Acquired

The government employs multiple safeguards that are designed to ensure that Section 702 collection is appropriately targeted at non-U.S. persons located outside the

conducted abroad. *Cf. Clapper*, 133 S. Ct. at 1149 (noting that the government conducts surveillance of persons abroad under "programs that are governed by Executive Order 12333" and that "[t]he Government may also obtain information from the intelligence services of foreign nations"); *Amnesty Int'l USA v. Clapper*, 667 F.3d 163, 192 (2d Cir. 2011) (Raggi, J., dissenting) (noting that because "the United States is hardly the only government conducting electronic surveillance," the foreign contacts of plaintiffs challenging the FAA might "be prime targets for surveillance by other countries," especially foreign contacts "believed to be associated with terrorist organizations"); *Verdugo*, 494 U.S. at 278 (Kennedy, J., concurring) (noting the relevance of "differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad"). This reality, which courts have acknowledged, arguably put the defendant "on notice . . . that some reasonable . . . intrusion on his privacy is to be expected." *King*, 133 S. Ct. at 1969.

⁷⁶ The cases cited by the defendant (Doc. 48 at 46) are not to the contrary. While *Warshak*, 631 F.3d at 282, held that a subscriber has a reasonable expectation of privacy in e-mails that the provider stores in the *subscriber's* account, it did not hold, much less suggest, that a person's Fourth Amendment rights are implicated when the government obtains, from the service provider, e-mails from *someone else's* account. The same is true of *In re Grand Jury Subpoena (Kitzhaber)*, 828 F.3d 1083, 1091 (9th Cir. 2016), which also involved a challenge by a user to the acquisition of communications from his own accounts. *Id.* at 1091 (concluding, based on terms of agreement with archiving agency, that former Oregon governor had reasonable expectation of privacy in contents of personal e-mails in his own Gmail accounts, but no such expectation with respect to e-mails transmitted through those accounts that concerned official business). Finally, *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), upheld the government's use of a pen register-like device to obtain addressing and routing information from the user's account; the contents of communications were not acquired. *See id.* at 505, 509-11.

United States for foreign intelligence purposes and to protect the privacy interests of persons located in the United States whose communications are incidentally collected. These safeguards and procedures—some of which go beyond what courts have held reasonable in the context of “special needs” warrantless searches involving less compelling governmental interests—provide constitutionally sufficient protection for the privacy interests of persons protected by the Fourth Amendment. *See Mohamud II*, 843 F.3d at 443 (holding that “the applicable targeting and minimization procedures, which were followed in practice, sufficiently protected [the defendant’s] privacy interest”).

i. Senior officials certify that the government’s procedures satisfy statutory requirements

Section 702 requires the DNI and the Attorney General to certify that procedures are in place to protect the privacy of persons located in the United States, including targeting procedures and minimization procedures. 50 U.S.C. § 1881a(a), (g), and (i). In addition, the Attorney General and the DNI must also certify, *inter alia*, that a significant purpose of the acquisition is to obtain foreign intelligence information, that they have adopted guidelines to ensure compliance with the statutory limitations in Section 702(b), and that the targeting procedures, minimization procedures, and guidelines adopted by the government are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A). The requirement that these senior executive branch officials certify that the procedures comply with statutory requirements and with the Constitution represents an important “internal check” on the actions of the Executive Branch. *See In re Sealed Case*, 310 F.3d at 739 (citation omitted).

ii. Prior Judicial review

Under Section 702, the government's certification, targeting procedures, and minimization procedures are all subject to FISC review. Section 702 requires the FISC to approve a certification if the court finds that it contains all the required elements and that the targeting and minimization procedures are consistent with 50 U.S.C. § 1881a(d) and (e) and with the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A). Prior FISC approval, and in particular the required judicial finding that the government's targeting and minimization procedures are consistent with the Fourth Amendment, supports the conclusion that Section 702 collection conducted pursuant to such procedures is constitutional. *See Clapper*, 133 S. Ct. at 1150 (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's declassified opinions make clear that the FISC subjects those procedures to exacting scrutiny. *See, e.g., Nov. 2015 FISC Op.* at 10-45; *[Caption Redacted]*, 2011 WL 10945618, at *5-28; *Sept. 2008 FISC Op.* at 32-41. Moreover, contrary to the defendant's assertion (Doc. 48 at 15, 41), "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." *Mem. Op.* at 3, *[Caption Redacted]* (FISA Ct. Aug. 26, 2014); *see also id.* at 25 ("The FISC has a continuing role in determining and enforcing compliance with these procedures.").⁷⁷

⁷⁷ Available at:

<https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf>.

iii. Targeting procedures ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States

Section 702 provides that the 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 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.” *See* 50 U.S.C. § 1881a(d)(1). The FISC repeatedly has found that the targeting procedures meet that standard. *See [Caption Redacted]*, 2011 WL 10945618, at *6 (“The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.”).

Targeting procedures generally⁷⁸ require the government to assess whether the potential target: (1) is a non-U.S. person; (2) reasonably believed to be located outside the United States (the “foreignness determination”); and (3) possesses and/or is likely to communicate or receive foreign intelligence information (the “foreign intelligence purpose determination”). PCLOB Report at 41-42. The foreignness determination is based on the totality of the circumstances. *Id.* at 43. If there is conflicting information regarding foreignness, that conflict must be resolved and the user must be determined

⁷⁸ This unclassified discussion of targeting procedures is derived from the PCLOB Report. The specific targeting procedures governing the Section 702 collection in this case remain classified and have been filed under seal with the Court. Certain recently declassified targeting procedures are available on the DNI’s website. *See* <https://icontherecord.tumblr.com> (“Release of the FISC Opinion Approving the 2016 Section 702 Certification and Other Related Documents”) (May 11, 2017).

to be a non-U.S. person reasonably believed to be located outside the United States. *Id.* at 44.

In making the foreign intelligence determination, the government must identify the specific foreign power or foreign territory about which the foreign intelligence is being sought. *Id.* at 45. Targeting procedures require documentation of the government's foreignness and foreign intelligence purpose determinations. *Id.* Targeting determinations by government analysts must be documented and are subject to an internal review process before the communications facility may be "tasked" for acquisition, and the tasking requests are also subject to oversight review by the Department of Justice and ODNI. *See id.* at 45-46.

Targeting procedures also require post-tasking analysis designed "to ensure that the users of tasked selectors remain non-U.S. persons located outside the United States" and "acquisition against the selector continues only insofar as the government assesses that the tasking is likely to acquire foreign intelligence information within one of the authorized Section 702 certifications." *Id.* at 48. If it is determined that a target reasonably believed to be outside the United States has since entered the United States, or that a person who at the time of targeting was believed to be a non-U.S. person was in fact a U.S. person, the acquisition must promptly be terminated. *Id.* at 49. Failure to de-task a Section 702 acquisition after it has been (or, based on available information, should have been) determined to be ineligible for further Section 702 acquisition is considered a compliance incident that must be reported first to the Department of Justice and ODNI, and then to the FISC and Congress. *Id.* Information

acquired as a result of an erroneous tasking or because of a failure to timely de-task a facility is subject to purge, with limited exceptions. *See id.*

Thus, under the targeting procedures, the government must first determine that the target is a non-U.S. person reasonably believed to be located outside the United States; the government may then obtain communications relating to specific identifiers, such as an e-mail address or telephone number, and only if the government determines that those identifiers are being used to communicate foreign intelligence information. *Id.* at 41; *see also Sept. 2008 FISC Op.* at 41 (holding that “the NSA’s assessment under its targeting procedures of the likelihood of obtaining foreign intelligence information provides a reasonable factual predicate for conducting the acquisitions”). These requirements limit the scope of the acquisition and support the reasonableness of the collection under Section 702.

iv. A significant purpose of the acquisition must be to obtain foreign intelligence information

Section 702 only authorizes collection when a significant purpose of the collection is to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A)(v). That requirement precludes the government from using directives under Section 702 “as a device to investigate wholly unrelated ordinary crimes.” *In re Sealed Case*, 310 F.3d at 736. The targeting procedures ensure that any surveillance satisfies this purpose by requiring an assessment that the individual or facility targeted for collection is likely to communicate foreign intelligence information. *See* PCLOB Report at 45; *see also In re Directives*, 551 F.3d at 1013 (finding that the “procedure[s] t[hat] ensure that a significant purpose of a surveillance is to obtain foreign intelligence

information” supported the constitutional reasonableness of the PAA); *Mohamud I*, 2014 WL 2866749, at *27 (same as to Section 702).

**v. Minimization procedures protect the privacy of
U.S. persons whose communications are acquired**

The government also employs minimization procedures, as defined in FISA, to limit the acquisition, retention, and dissemination of information concerning U.S. persons consistent with the government’s foreign intelligence needs.⁷⁹ See 50 U.S.C. § 1801(h)(1); PCLOB Report at 50 (“Minimization procedures are best understood as a set of controls on data to balance privacy and national security interests.”). Section 702 further requires that the FISC review those procedures and determine that acquisitions in accordance with such procedures would be consistent with the FAA and the Fourth Amendment. 50 U.S.C. § 1881a(i)(1) and (2). All Section 702-acquired information is subject to the FISC-approved minimization procedures.

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

⁷⁹ This unclassified discussion of minimization procedures is derived from the PCLOB Report. The specific minimization procedures governing the Section 702 collection in this case remain classified and have been filed under seal with the Court. Certain declassified minimization procedures used by the NSA, FBI, and CIA are available on the DNI’s website. See <https://icontherecord.tumblr.com> (“Release of the FISC Opinion Approving the 2016 Section 702 Certification and Other Related Documents”) (May 11, 2017); <https://icontherecord.tumblr.com/tagged/declassified/page/3> (“Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act”) (Sept. 29, 2015).

PCLOB Report at 64-66. As the FISC has held, the minimization procedures ensure that any intrusion on the privacy of U.S. persons is reasonably balanced against the government's intelligence needs. *See, e.g., Sept. 2008 FISC Op.* at 40.

Procedures governing Section 702 collection generally parallel procedures employed for FISA Title I and III collection, as well as the PAA procedures. The FISA Court of Review has found that these procedures sufficiently protect the privacy interests of U.S. persons whose communications are incidentally acquired and that such procedures are an important factor in upholding the constitutional reasonableness of traditional FISA surveillance and the PAA. *See In re Sealed Case*, 310 F.3d at 740-41; *see In re Directives*, 551 F.3d at 1015 (finding it “significant” 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.”). For the same reasons that courts have found the use of minimization procedures to be an important factor in holding traditional FISA surveillance to be reasonable under the Fourth Amendment, the use of substantially similar minimization procedures supports the reasonableness of surveillance under Section 702. *See Mohamud I*, 2014 WL 2866749, at *23 (holding that “the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment”); *see also Sept. 2008 FISC Op.* at 29-32, 40 (recognizing that the applicable minimization procedures closely resemble those used in traditional FISA surveillance and physical search that the FISC had repeatedly upheld, and that the

relatively slight differences did not undermine the procedures' compliance with the statute or the Fourth Amendment).

The defendant argues (Doc. 48 at 5, 15, 41) that minimization is inadequate because the FISC has "no power" to supervise the government's compliance with minimization procedures. However, Section 702's oversight provisions require regular reporting to the FISC concerning the government's implementation of minimization procedures. 50 U.S.C. § 1881a(1). In addition, Rule 13 of the FISC's Rules of Procedures requires the government to report, in writing, all instances of non-compliance. See FISC R. 13(b); see also PCLOB Report at 75-76 (describing the FISC's role in providing continuous oversight of the government's compliance with Section 702 requirements, including the FISC's continuing authority to "seek additional information, issue orders to the government to take specific action to address an incident of noncompliance, or (if deemed necessary) issue orders to the government to cease an action that the court assesses to be non-compliant"). The FISC also has authority to disapprove or to require amendments to the minimization procedures, as indeed, the FISC has done.⁸⁰

⁸⁰ In *[Caption Redacted]*, 2011 WL 10945618, at *1, the FISC found that the government's minimization procedures, as applied to certain electronic communications acquired at "upstream" points on the internet backbone networks, did not comply with Section 702 or the Constitution, due to technical limits on the government's ability to isolate targeted communications that were transmitted as part of a multi-communication batch. The government revised its procedures, and the FISC held that the amended procedures were consistent with the statute and the Fourth Amendment. *[Caption Redacted]*, 2011 WL 10947772, at *1.

As noted above, there is no "upstream" collection at issue in this case.

The defendant further contends (Doc. 48 at 40-41, 48-52) that the minimization procedures are inadequate because they permit the government to query information already collected pursuant to Section 702 using terms associated with U.S. persons. See PCLOB Report at 55-60 (discussing querying practices permitted under each agency's minimization procedures).⁸¹ That contention lacks merit.

[CLASSIFIED MATERIAL REDACTED]

In any event, courts have held in various contexts that where the government's querying of information that has lawfully been obtained does not implicate any reasonable expectation of privacy beyond that implicated in the initial collection, merely running queries in a database does not infringe on any significant privacy interest or trigger any fresh constitutional analysis. See *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 an expectation of privacy that society is prepared to recognize as reasonable, 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) (holding that "accessing the records stored in the [DNA] database is not a 'search' for Fourth Amendment purposes" based in part on cases holding that, where a photograph is "taken in conformance with the Fourth Amendment, the government's storage and use of it does not give rise to an independent Fourth Amendment claim"). The Sixth Circuit has applied this principle in the foreign intelligence context. See *Jabara v. Webster*, 691 F.2d 272, 277-79 (6th

⁸¹ **[CLASSIFIED MATERIAL REDACTED]**

Cir. 1982) (holding, where plaintiff did not challenge the lawfulness of warrantless NSA interception of his foreign communications but challenged only the subsequent dissemination of the communications to the FBI, that such dissemination “after the messages had lawfully come into the possession of the NSA” did not implicate any reasonable expectation of privacy).⁸²

The same reasoning applies here. Where the government has lawfully collected foreign intelligence information pursuant to statutory requirements and FISC-approved procedures that meet Fourth Amendment standards, the government’s subsequent querying of that information does not amount to a significant further intrusion on privacy that implicates the Fourth Amendment. *See King*, 133 S. Ct. at 1980 (holding, “in light of the scientific and statutory safeguards” governing Maryland’s warrantless collection of DNA from persons arrested for serious offenses, that “once respondent’s DNA was lawfully collected,” the subsequent analysis of the DNA “did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment”). Accordingly, contrary to the defendant’s assertion (Doc. 48 at 48-52), the government’s querying (whether using U.S. person identifiers or otherwise) of information lawfully obtained pursuant to

⁸² A rule that every query, dissemination, or use of Section 702-obtained information amounts to a separate search under the Fourth Amendment would not only be contrary to these cases but also would be impracticable, because, as the Sixth Circuit explained in *Jabara*, such a rule would require “a succession of warrants as information, lawfully acquired, is passed from one agency to another.” 691 F.2d at 279; *see also id.* at 277 (“Evidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken.”) (citation omitted). Accordingly, “an expectation that information lawfully in the possession of a government agency will not be disseminated, without a warrant, to another government agency is [not] an expectation that society is prepared to recognize as reasonable.” *Id.* at 279.

Section 702 does not amount to a separate search under the Fourth Amendment and does not require separate or additional judicial process, as other courts have correctly held. *See Mohamud I*, 2014 WL 2866749, at *24-26; *Hasbajrami*, 2016 WL 1029500, at *12 n.20; *Muhtorov*, slip op. at 31.⁸³

A U.S. person query, whether for foreign intelligence or a criminal investigation, is not a search that exceeds the original foreign intelligence justification for the collection. Foreign intelligence must be a “significant” purpose under Section 702, but it need not be the exclusive purpose. *In re Sealed Case*, 310 F.3d at 742-43. All of the information queried using a U.S. person identifier falls within the scope of a FISC-approved foreign intelligence certification. By analogy, if a DEA agent lawfully seizes a drug ledger that also reveals evidence of tax evasion, there is no legal requirement that the IRS obtain a separate warrant to examine the properly seized drug ledger; moreover, the fact that more than one person used the drug ledger also creates no additional requirement that the government seek a warrant or other legal justification to examine the document. *See, e.g., Maryland v. Garrison*, 480 U.S. 79, 86 (1987). In any event, this case involves an investigation of criminal conduct relating to international terrorism, and evidence of such crimes falls squarely within FISA’s definition of “foreign intelligence information.” *See In re Sealed Case*, 310 F.3d at 724.

⁸³ Insofar as the defendant requests (Doc. 48 at 52) an order prospectively requiring the government to obtain individualized court approval before making U.S. person queries of Section 702-acquired information, that request should be rejected, both because, as established in the text above, the government’s existing querying practices are lawful, and because such an order would exceed this Court’s authority in adjudicating a motion to suppress under 50 U.S.C. § 1806.

Nor do procedures permitting the government to query information lawfully collected pursuant to Section 702 using identifiers associated with U.S. persons render the minimization procedures constitutionally unreasonable. As noted above, the querying of information that the government lawfully has obtained is not a significant additional intrusion on a person's privacy, beyond the level of intrusion that has already resulted from the government's collection and review of the information pursuant to court-approved targeting and minimization procedures. Consistent with those procedures, the government is of course permitted 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 the FISC-approved minimization procedures. It would be perverse to authorize the unrestricted review of lawfully collected information but then to restrict the targeted review of the same information in response to tailored queries. *Hasbajrami*, 2016 WL 1029500, at *12 n.20; *see also* PCLOB Report at 131 (“[R]ules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence or, in the FBI’s case, for evidence of a crime.”).

On the other side of the balance, the government has a powerful interest in conducting such queries for appropriate purposes including, for example, discovering potential links between foreign terrorist groups and persons within the United States

in order to detect and disrupt terrorist activity. See Part IV.A.3.⁸⁴ Similarly, the government's interest in preventing crime is "paramount," and a criminal investigation is always a "compelling" state interest. *Branzburg v. Hayes*, 408 U.S. 665, 700 (1972); see also *In re Directives*, 551 F.3d at 1011 ("A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose" because, for example, the "apprehension of terrorism suspects . . . is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection.").

The FISC repeatedly has approved minimization procedures that permit queries using U.S. person identifiers. See *[Caption Redacted]*, 2011 WL 10945618, at *7.⁸⁵ Indeed, the FISC recently conducted a thorough reexamination of the querying provisions of the Section 702 minimization procedures and concluded that the government's querying practices are consistent with the requirements of the statute

⁸⁴ Such queries also help the government counteract operational security measures such as hiding operational communications in large amounts of non-operational communications in the hope of delaying the government's detection of the operational communications.

⁸⁵ The FISC has long approved the querying of FISA Title I data, including with U.S. person identifiers, when such queries are designed to yield foreign intelligence information or evidence of a crime. Indeed, in approving such queries in the context of Section 702 collection, the FISC has noted that the minimization procedures applicable to information acquired through Title I and III of FISA, which the FISC had previously approved, similarly permit queries using U.S. person identifiers, even though that information was likely to include a higher concentration of U.S. person information than Section 702 collection. See *[Caption Redacted]*, 2011 WL 10945618, at *7. The FISC concluded, "[i]t follows that the substantially-similar querying provision found [in] the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons." *Id.*

Likewise, for decades the minimization procedures of the federal Wiretap Act have specifically allowed the government to search for and use evidence from a wiretap to prove a crime unrelated to the original purpose for the wiretap. See 18 U.S.C. § 2517(5); see also, e.g., *United States v. Goffer*, 721 F.3d 113, 124 (2d Cir. 2013).

and the Fourth Amendment. *See, e.g., Nov. 2015 FISC Op.* at 24-36, 39-45. Because the government's querying of information lawfully acquired under Section 702 pursuant to the court-approved minimization procedures is reasonable under the Fourth Amendment, this Court should reach the same conclusion.⁸⁶

vi. Executive Branch, Congressional, and Judicial oversight

The Section 702 program is subject to extensive oversight by all three branches of government. *See* PCLOB Report at 66-79 (detailing the various forms of internal and external oversight). Section 702 requires the Attorney General and the DNI to periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines. *See* 50 U.S.C. § 1881a(l). They must submit those assessments both to the FISC and to congressional oversight committees. *Id.* The Attorney General must also keep the relevant oversight committees "fully inform[ed]" concerning the implementation of Section 702. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment.").

In 2012, the Senate Select Committee on Intelligence ("SSCI"), following four years of such oversight, found:

[T]he assessments, reports, and other information obtained by the Committee demonstrate that the government implements the FAA surveillance authorities in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have

⁸⁶ [CLASSIFIED MATERIAL REDACTED]

been promptly reported and remedied. Through four years of oversight, the Committee has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law. Moreover, having reviewed opinions by the FISA Court, the Committee has also seen the seriousness with which the Court takes its responsibility to carefully consider Executive Branch applications for the exercise of FAA surveillance authorities.

S. Rep. No. 112-174, at 7 (2012); *see also* H.R. Rep. No. 112-645, pt. 2, at 4 (2012) (“The oversight this Committee has conducted since the FAA was enacted in 2008 has shown no evidence that the Intelligence Community has engaged in any intentional or willful failure to comply with statutory requirements or Executive Branch policies and procedures.”); *see also* PCLOB Report at 11 (“The Board has seen no trace” of any attempted “exploitation of information acquired under [Section 702] for illegitimate purposes” nor “any attempt to intentionally circumvent legal limits.”). Under the FAA, as in traditional FISA, the “in-depth oversight of FISA surveillance by all three branches of government” helps to “ensure[]” the “privacy rights of individuals” and to “reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.” *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982).

The compliance incidents identified by the defendant (Doc. 48 at 23-24 & n.21, 33 n.23) fail to support his constitutional challenge. The rate of compliance incidents under the Section 702 program is extremely low. *See* PCLOB Report at 77-78 (noting that the “incident rate has been substantially below one percent since the Section 702 program was initiated”). A large proportion of the incidents that have occurred have no privacy implications. *See id.* at 78 (noting that more than half of the incidents have

occurred in cases in which the targeting and minimization procedures were otherwise followed, but NSA was untimely in making reports regarding proper taskings or de-taskings to the Department of Justice or ODNI). And, as the SSCI concluded, when problems have arisen, they have been “promptly reported and remedied,” in large part because of the robust oversight discussed above. S. Rep. No. 112-174, at 7. With one exception, the incidents that have occurred have not precluded the FISC from concluding that the targeting and minimization procedures, as written and implemented, are consistent with the statutory requirements and the Fourth Amendment. And in that one instance, the government promptly cured the procedural deficiency that had been identified by the FISC. *See [Caption Redacted]*, 2011 WL 10947772, at *1.

d. Collection Under Section 702 Has Sufficient Particularity

The defendant’s overarching argument is, in essence, that collection pursuant to Section 702 fails the Fourth Amendment’s general reasonableness test because it does not require a particularized court order or finding of probable cause as in traditional FISA collection or domestic law enforcement wiretaps. *See* Doc. 48 at 27-41. In making this argument, the defendant characterizes Section 702-authorized collection as “dragnet” surveillance that collects communications in “bulk.” *See, e.g., id.* at 13, 34, 38. However, collection under Section 702 is *not* bulk collection. *See* PCLOB Report at 111 (“[T]he Section 702 program is not based on the indiscriminate collection of information in bulk” because “the program consists entirely of targeting specific persons about whom an individualized determination has been made.”); *see also id.* at

103 (“The [Section 702] program does not operate by collecting communications in bulk.”).

Section 702 collection is focused and reasonable because FISC-approved procedures require the government to determine: (1) that the particular “user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States,” *[Caption Redacted]*, 2011 WL 10945618, at *7; and (2) the collection is designed to obtain foreign intelligence information within the scope of the certification approved by the court. *See Sept. 2008 FISC Op.* at 39 n.47 (finding it “obvious” that “communications to and from targets identified under these [targeting] procedures would be expected to contain foreign intelligence information”); *Mem. Op.* at 26, *[Caption Redacted]* (FISA Ct. Aug. 26, 2014) (“While in absolute terms, the scope of acquisitions under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner.”). Thus, as the PCLOB noted, 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 e-mail address or telephone number, and the government acquires only communications involving that particular selector. PCLOB Report at 20-23, 32-33, 111-12.

[CLASSIFIED MATERIAL REDACTED]

Moreover, the defendant’s argument conflates the test for constitutional reasonableness with the *different* requirements for a warrant under the Fourth Amendment. *See* U.S. Const. amend IV (“[N]o warrants shall issue, but upon probable

cause, supported by Oath or Affirmation, *and particularly describing the place to be searched*") (emphasis added). In *In re Directives*, the FISA Court of Review rejected the petitioner's "invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable." 551 F.3d at 1013.

Although particularity may be considered as one factor among many in assessing the reasonableness of a particular search, the Fourth Amendment "imposes no irreducible requirement" of individualized suspicion where the search is otherwise reasonable, as it is here. *See King*, 133 S. Ct. at 1969. Moreover, as the FISA Court of Review found in the context of the PAA, the "matrix of safeguards," including robust targeting and minimization procedures, provide constitutionally sufficient protections for the same interests that would be served by requirements of particularity or prior judicial review of individual targets. *In re Directives*, 551 F.3d at 1013.

In sum, in enacting Section 702, Congress and the Executive Branch developed a framework of procedures to facilitate the collection of foreign intelligence vital to the nation's security while protecting any constitutionally protected privacy interests implicated by the collection. That framework is entitled to the utmost constitutional respect by this Court. *See Youngstown*, 343 U.S. at 635-37 (Jackson, J., concurring); *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."). The safeguards built into the statute and the certification(s) and procedures which were implemented here ensured that the

collection targeted only foreign person(s) outside the United States and was conducted in a way that only incidentally implicated the privacy of persons located in the United States.

Evaluating the totality of the circumstances and weighing the compelling governmental interests at stake in combination with the extensive safeguards employed by the government to protect the privacy interests of persons protected by the Fourth Amendment, this Court should hold that the government's acquisition pursuant to Section 702 of the foreign intelligence information challenged by the defendant meets the Fourth Amendment's central requirement of reasonableness.⁸⁷

B. SECTION 702 IS CONSISTENT WITH ARTICLE III

The defendant contends (Doc. 48 at 41-44) that the FISC does not perform a proper judicial role under Article III in reviewing targeting and minimization procedures pursuant to Section 702 because the court does not review the procedures in the context of a particular proposed target and interception. The defendant further maintains that review at this level of generality does not present a "case or controversy" within the meaning of Article III. Those contentions have no merit, as the Ninth Circuit recently concluded. *See Mohamud II*, 843 F.3d at 444 n.28.

"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); *see also Morrison v. Olson*, 487 U.S. 654, 679 n.16

⁸⁷ Although the defendant is not a U.S. person, the safeguards discussed above are also reasonable and adequate as to him. *See* PCLOB Report at 98-100 (discussing the various ways non-U.S. persons are afforded privacy protection under the Section 702 program).

(1988). In particular, the courts have long participated in the oversight of government searches and surveillance by reviewing warrant and wiretap applications, notwithstanding that these proceedings are wholly *ex parte* and do not occur at the behest of an aggrieved party as ordinarily required for a “case or controversy” under Article III. *Mistretta*, 488 U.S. at 389 n.16; *see also, e.g., In re Sealed Case*, 310 F.3d at 732 n.19 (“In light of [*Morrison* and *Mistretta*], we do not think there is much left to an argument . . . that the statutory responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process.”); *In re Kevork*, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985), (regarding the practices under previous SMPs), *aff’d*, 788 F.2d 566 (9th Cir. 1986).⁸⁸

Congress, in assigning the FISC an analogous function in Section 702, did not vest the FISC with a power that is “incongruous” with the judicial function or that “more appropriately belong[s] to another Branch” – the central question in a separation of powers challenge under Article III. *Mistretta*, 488 U.S. at 390; *see also In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 144 (E.D. Va. 2011) (“Grand Juries, search warrants, wiretap orders, and many other *ex parte* applications and orders rely on judicial review to protect the rights of potential subjects of investigation. All of these tools have been routinely and consistently approved by the courts.”). Congress’s decision to vest the FISC with

⁸⁸ The judiciary participates in oversight of searches and seizures not only by reviewing applications and issuing warrants, but also through its participation in promulgating the procedural rules governing the warrant process. *See* Fed. R. Crim. P. 41; *Mistretta*, 488 U.S. at 387-88 (noting that Congress may properly delegate to the courts the authority to prescribe rules of procedure in criminal cases).

jurisdiction to review the reasonableness of procedures for searches or surveillance under Section 702 is perfectly 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. *Cf. Mistretta*, 488 U.S. at 390-91 (given the judiciary's traditional role in determining individual criminal sentences, the judiciary could constitutionally participate in formulating general sentencing guidelines). The court in *Mohamud II* correctly rejected the same Article III arguments that the defendant raises here, explaining that the FISC's "[r]eview 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." 843 F.3d at 444 n.28 (internal quotation marks omitted).

Moreover, the decision the FISC is called upon to render under Section 702 is not merely "advisory," any more than a decision on a traditional search warrant or wiretap application is "advisory." If the FISC disapproves the government's proposed targeting or minimization procedures under Section 702, that decision has legal effect, because it bars the government from conducting collections under the statute if it does not remedy the deficiency within thirty days. A FISC order approving the proposed certification and procedures also has an effect on third parties, because it authorizes the government to issue directives (compulsory process analogous to a subpoena) to electronic communications service providers. The fact that the providers have a right to challenge such a directive in court further establishes that a FISC order approving a Section 702 certification is not an advisory opinion but a legally enforceable order

potentially subject to legal challenge. *See Clapper*, 133 S. Ct. at 1154 (“[A]ny electronic communications service provider that the Government directs to assist in § 1881a surveillance may challenge the lawfulness of that directive before the FISC.”); *Mohamud I*, 2014 WL 2866749, at *11 (rejecting defendant’s argument that “FISC judges only provide advisory opinions”).

The defendant is also incorrect in claiming (Doc. 48 at 43) that the lack of a particular factual context for the FISC’s review of the government’s certification renders the issue inappropriate for resolution by an Article III judge. Even the principal case on which he relies 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.

Section 702 requires the FISC to review specific targeting and minimization procedures to determine whether they comply with applicable statutory standards and the Fourth Amendment. That review is not conducted in the abstract; rather, the FISC must review the minimization procedures “in light of the purpose and technique of the *particular* surveillance.” 50 U.S.C. § 1801(h)(1) (emphasis added); *see also id.* § 1821(4)(A) (requiring that minimization procedures with respect to physical search must be “reasonably designed in light of the purposes and technique of the *particular* physical search”) (emphasis added). Accordingly, the FISC’s review must consider the particular “purpose,” as set forth in the certification, of the acquisitions, as well as the particular “technique[s]” the government uses. This often involves a close

consideration of the application of specific, detailed provisions in the targeting and minimization procedures as applied to specific, technical tools through which the government implements Section 702. *See [Caption Redacted]*, 2011 WL 10945618, at *9 (“The Court has repeatedly noted that the government’s targeting and minimization procedures must be considered in light of the communications actually acquired.”). That level of particularity and detail is exemplified in the declassified FISC opinions addressing the adequacy of particular targeting and minimization procedures in the context of certain technical limitations in the NSA’s “upstream collection” of Internet communications transmitted as part of a multi-communication batch. *See id.* at *9-10.

Analyzing the reasonableness of electronic surveillance, in light of the government’s national security interests and the privacy interests of potential subjects of the surveillance, is a traditional judicial function. *See Halperin v. Kissinger*, 606 F.2d 1192, 1201 n.59 (D.C. Cir. 1979) (“[D]etermin[ing] whether electronic surveillance was consonant with statutory and constitutional strictures [is] a traditional judicial function that is governed by well established and manageable standards.”). The closely related question of whether surveillance conducted pursuant to particular procedures is reasonable under the relevant statutory and constitutional standards is also the kind of analysis that courts regularly undertake, such as, for example, when they adjudicate the constitutionality of a state statute regulating domestic wiretaps. *See United States v. Tortorello*, 480 F.2d 764, 772-73 (2d Cir. 1973) (analyzing constitutional adequacy of procedures provided by New York electronic surveillance statute).

The FISC's role under Section 702 is also analogous to judicial review of administrative warrants in the public health context, which may be based on the court's determination of the reasonableness of the standards and procedures for conducting inspections in a given area, rather than evidence of a violation at a specific location. *See Camara v. Municipal Ct.*, 387 U.S. 523, 537-38 (1967) ("Such standards, which will vary with the municipal program being enforced, may be based upon the passage of time, the nature of the building (*e.g.*, a multifamily apartment house), or the condition of the entire area, but they will not necessarily depend upon specific knowledge of the condition of the particular dwelling."). 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 anything in Article III.

C. THE GOOD FAITH EXCEPTION APPLIES

The good-faith exception to the exclusionary rule set forth in *United States v. Leon*, 468 U.S. 897, 913 (1984), provides an independent basis for denying the defendant's suppression motion. *See, e.g., United States v. Ning Wen*, 477 F.3d 896, 897-98 (7th Cir. 2007) (applying good-faith exception to a claim that FISA surveillance violated the Fourth Amendment). The good-faith rule applies when law enforcement agents act in "objectively reasonable reliance on a statute" authorizing warrantless searches that are later deemed unconstitutional, *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987), when law enforcement officers reasonably rely on the probable-cause determination of a neutral magistrate, *see Leon*, 468 U.S. at 920, and when law

enforcement officers reasonably rely on then-binding appellate precedent that is subsequently overturned, *see Davis v. United States*, 564 U.S. 229, 249 (2011).

The good-faith exception applies here because the collection at issue was authorized by a duly enacted statute, an order issued by a neutral magistrate, and court of appeals precedent. *Mohamud I*, 2014 WL 2866749, at *30 (holding that the good-faith exception applies to Section 702 surveillance conducted in reliance on the statute and a FISC-approved certification). First, government agents conducted the collection at issue here pursuant to Section 702, as well as under procedures adopted by the Attorney General pursuant to the statute. *See Krull*, 480 U.S. at 349; *Duka*, 671 F.3d at 346 (reasoning that the good-faith rule applies because the search was conducted in “objectively reasonable reliance” on a duly authorized statute—*i.e.*, FISA); *see also United States v. Marzook*, 435 F. Supp. 2d 778, 790-91 (N.D. Ill. 2006) (holding that “the FBI’s reliance on the Attorney General’s approval under Executive Order 12333—an order that no court has found unconstitutional—was [] objectively reasonable because that order pertains to foreign intelligence gathering”). Second, the agents also reasonably relied on order(s) issued by neutral magistrates—the judges of the FISC—who repeatedly have held that the applicable targeting and minimization procedures are reasonable under the Fourth Amendment. *See Leon*, 468 U.S. at 920; *see also Duka*, 671 F.3d at 347 n.12 (“[O]bjective . . . reliance on the statute in this case is further bolstered by the fact that the particular provision at issue has been reviewed and declared constitutional by several courts.”); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 140 n.12 (D. Mass. 2007) (applying the good-faith exception because

“there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders”). Finally, the agents reasonably relied on appellate precedent from the FISA Court of Review that upheld similar directives issued under the PAA. *See Davis*, 564 U.S. at 247-49; *In re Directives*, 551 F.3d at 1016.

The defendant cannot show that Section 702 is so “clearly unconstitutional,” *Krull*, 480 U.S. at 349, that “a reasonable officer should have known that the statute was unconstitutional,” *id.* at 355. Nor can they show that the collection was the result of “systemic error or reckless disregard of constitutional requirements.” *Herring v. United States*, 555 U.S. 135, 147 (2009). Accordingly, even if the collection were deemed unconstitutional, the evidence derived from that collection would not be subject to exclusion.⁸⁹

⁸⁹ In the related context of Title III of the Wiretap Act, the weight of the precedent establishes that Title III’s statutory suppression remedy for criminal wiretap orders incorporates the good-faith exception. *See United States v. Moore*, 41 F.3d 370, 374, 376 (8th Cir. 1994) (applying good-faith exception to Title III violation); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988) (same); *United States v. Brewer*, 204 F. App’x 205, 208 (4th Cir. 2006) (same); *United States v. Solomonyan*, 451 F. Supp. 2d 626, 637-38 (S.D.N.Y. 2006) (collecting cases). Although two courts of appeals have held otherwise, both courts also questioned in those cases whether the government’s actions were actually taken in “good faith,” either because the affiant recklessly misled the court, *see United States v. Rice*, 478 F.3d 704, 709-11 (6th Cir. 2007); or because the wiretap order, in the court’s view, plainly violated the applicable rule, *see United States v. Glover*, 736 F.3d 509, 515-16 (D.C. Cir. 2013). In this case, even if some aspect of the collection did not comply with the requirements of Section 702, there is no similar indication of deliberate, reckless, or systemically negligent conduct. Accordingly, absent a finding that the government personnel who carried out the collection did not rely in good faith on the targeting and minimization procedures as approved by the FISC, or otherwise engaged in culpable conduct warranting application of the exclusionary rule, the defendant’s motion to suppress should be denied.

**V. THE SECTION 702 INFORMATION WAS LAWFULLY ACQUIRED
AND ACQUISITIONS WERE CONDUCTED IN CONFORMITY WITH
ORDER(S) OF AUTHORIZATION OR APPROVAL**

[CLASSIFIED MATERIAL REDACTED]

A. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

**B. THE APPLICABLE TARGETING PROCEDURES MET THE
STATUTORY REQUIREMENTS**

[CLASSIFIED MATERIAL REDACTED]

**C. THE APPLICABLE MINIMIZATION PROCEDURES MET THE
STATUTORY REQUIREMENTS**

[CLASSIFIED MATERIAL REDACTED]

D. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

1. Relevant Facts

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

4. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

VI. THE TITLE III FISA INFORMATION WAS LAWFULLY ACQUIRED AND
THE PHYSICAL SEARCH WAS MADE IN CONFORMITY WITH
ORDER(S) OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED]

A. STANDARD OF REVIEW

In evaluating the legality of the traditional FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(f), 1825(g).

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded due deference, the material under review here satisfies either standard of review. *See Abu-Jihaad*, 630 F.3d at 130 (“Although the established standard of judicial review applicable to FISA warrants is deferential, the government’s detailed and complete submissions in this case would easily allow it to clear a higher standard of review.”); *accord United States v. Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007, at *21-22 (N.D. Ga. Mar. 19, 2009) (FISC’s “determination of probable cause should be given ‘great deference’ by the reviewing court”) (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983)).⁹⁰

⁹⁰ A majority of federal courts have determined that the probable cause determination of the FISC should be reviewed *de novo*. *See United States v. Kashmiri*, No. 09-CR-830-4, 2010 WL 4705159, at *1 (N.D. Ill. Nov. 10, 2010); *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev’d on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006); *United States v. Warsame*, 547 F. Supp. 2d 982, 990-91 (D. Minn. 2008) (explaining the required showing is “a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability” that the search will be fruitful (citing *Gates*, 462 U.S. at 238)); *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, *5-6 (D. Or. Apr. 21, 2010). In each of these cases, the courts applied a *de novo* standard in reviewing the FISC’s probable cause findings, and each court found the applications before it contained probable cause.

1. Probable Cause Standard

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. It is this standard – not the standard applicable to criminal search warrants – that this Court must apply. *See El-Mezain*, 664 F.3d at 564 (“[t]his probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power”); *Abu-Jihaad*, 630 F.3d at 130; *Duka*, 671 F.3d at 338; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *Keith*, 407 U.S. at 322). This different standard “reflects the purpose for which FISA search orders are issued.” *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *22.

2. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be “subjected only to minimal scrutiny by the courts,” *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are “presumed valid.” *United States v. Duggan*, 743 F.2d 59, 77 & n.6 (2d Cir. 1984) (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) (“a presumption of validity [is] accorded to the certifications”); *Nicholson*, 2010 WL 1641167, at *5 (quoting *Rosen*, 447 F. Supp. 2d at 545); *Warsame*,

547 F. Supp. 2d at 990 (“a presumption of validity [is] accorded to the certifications”). When a FISA application is presented to the FISC, “[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official’s certification that the objective of the surveillance is foreign intelligence information.” *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should “have no greater authority to second-guess the executive branch’s certifications than has the FISA judge.” *Id.*; see also *In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *United States v. Rahman*, 861 F. Supp. 247, 250 (S.D.N.Y. 1994); *United States v. Islamic Am. Relief Agency (IARA)*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009); *Kashmiri*, 2010 WL 4705159, at *1.

The district court’s review should determine whether the certifications were made in accordance with FISA’s requirements and, when the target is a United States person, that each certification is not “clearly erroneous.” See *Kashmiri*, 2010 WL 4705159, at *2; *United States v. Alwan*, No. 1:11-CR-13-R, 2012 WL 399154, at *7 (W.D. Ky. Feb. 7, 2012) (“the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made”) (quoting *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *20); see also *Campa*, 529 F.3d at 993-94 (“in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target”); *Duggan*, 743 F.2d at 77. A “clearly erroneous” finding is established only when “although there is evidence to support [the issuing court’s conclusion], the reviewing court on the [basis of the] entire evidence is left with the definite and firm

conviction that a mistake has been committed.” *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 WL 5169536, at *4 (identifying “clearly erroneous” standard of review for FISA certifications).

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

C. THE INSTANT FISA APPLICATION(S) MET FISA’S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

4. **Conclusion: There Was Sufficient Probable Cause to Establish that the Information Acquired from the Targeted Facilities, Places, Property, or Premises Was Lawfully Acquired**

[CLASSIFIED MATERIAL REDACTED]

D. THE CERTIFICATIONS IN THE APPLICATION(S) COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED]

1. **Foreign Intelligence Information**

[CLASSIFIED MATERIAL REDACTED]

2. **“A Significant Purpose”**

[CLASSIFIED MATERIAL REDACTED]

3. **Information Not Reasonably Obtainable Through Normal Investigative Techniques**

[CLASSIFIED MATERIAL REDACTED]

E. PHYSICAL SEARCH WAS CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED]

1. **The Standard Minimization Procedures**

Once a reviewing court is satisfied that the physical search was properly certified and the information was lawfully acquired pursuant to FISA, it must then examine whether the physical search was lawfully conducted. *See* 50 U.S.C. § 1825(f)(1)(B). In order to examine whether the physical search was lawfully

conducted, the reviewing court must determine whether the government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED]

In reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an “objective assessment of the [agents’] actions in light of the facts and circumstances confronting [them] at the time.” *Scott v. United States*, 436 U.S. 128, 136 (1978). “The test of compliance is ‘whether a good faith effort to minimize was attempted.’” *Mubayyid*, 521 F. Supp. 2d at 135; *see also Hammoud*, 381 F.3d at 334 (“[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information”); *see* S. Rep. No. 95-701, at 39-40 (1978) (stating that the court’s role is to determine whether “on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion”); *IARA*, 2009 WL 5169536, at *6 (quoting S. Rep. No. 95-701, at 39-40).

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED]

VII. THE DEFENDANT'S MOTIONS FOR ADDITIONAL NOTICE AND DISCOVERY SHOULD BE DENIED

The defendant seeks notice and disclosure of any information collected pursuant to E.O. 12333 (Doc. 51, at 1), as well as “notice and discovery of all the surveillance techniques that the government used” in this case, citing to the Fourth, Fifth, and Sixth Amendments to the Constitution, 18 U.S.C. § 3504, and F.R.C.P. 12 and 16.⁹¹ (Doc. 52, at 7). As the Court will see from its *in camera*, *ex parte* review of the FISA materials, and for the reasons stated below, the government has complied with its notice and discovery obligations, and thus, the defendant’s motions lack merit and should be denied.

The government’s discovery obligations in a criminal case are not limitless. *See United States v. Agurs*, 427 U.S. 97, 106 (1976) (the government is under “no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor”); *United States v. Phillips*, 854 F.2d 273, 277 (7th Cir. 1988) (finding that discovery rules do “not grant criminal defendants unfettered access to government files”); *United States v. Griebel*, 312 F. App’x 93, 96 (10th Cir. 2008) (the government’s discovery obligations “are defined by Rule 16, *Brady*, *Giglio*, and the Jencks Act”); *United States v. Colon*, No. 97-CR-659, 1998 WL 214714, at *7-9 (N.D. Ill. Apr. 21, 1998) (addressing the government’s discovery obligations). Further, there is no rule of discovery that requires the government to provide a defendant with a clear, concise narrative regarding the origins of the criminal investigation that led to his arrest. *See*

⁹¹ [CLASSIFIED MATERIAL REDACTED]

Pennsylvania v. Ritchie, 480 U.S. 39, 59 (1987) (“defendant’s right to discover exculpatory evidence does not include the unsupervised authority to search through the [government’s] files”); *United States v. Bagley*, 473 U.S. 667, 675 (1985) (“the prosecutor is not required to deliver his entire file to defense counsel”). Rather, the government is required to provide the defense with all discoverable material (including exculpatory information) described in F.R.C.P. 16.

Notice concerning the government’s intent to use evidence in a criminal case is generally governed by F.R.C.P. 12 and 16. F.R.C.P. 12(b)(4)(B) provides in relevant part:

[T]he defendant may, in order to have an opportunity to move to suppress evidence under Rule 12(b)(3)(C), request notice of the government’s intent to use (in its evidence-in-chief at trial) any evidence that the defendant may be entitled to discover under Rule 16.

The purpose of this rule is to “provide the defendant with sufficient information to file the necessary suppression motions.” *United States v. Ishak*, 277 F.R.D. 156, 158 (E.D. Va. 2011). “Thus, the government’s obligation under Rule 12(b)(4)(B) ends when it has made disclosures that sufficiently allow the defendant to make informed decisions whether to file one or more motions to suppress.” *Id.* The government has satisfied this obligation and provided the defendant with sufficient information and notice to file any necessary motions to suppress. No court has interpreted F.R.C.P. 12(b)(4)(B) to require the government to give an accounting of every investigative technique used in the case, regardless of its relationship to admissible evidence. In a criminal case, defense counsel analyzes the discovery, determines what suppression motions to make,

and files them. The government then responds. That is precisely what has occurred in the instant case. For these reasons, the defendant's request for more information than any rule or statute requires should be denied.

The government's notice obligations regarding the use of FISA information under 50 U.S.C. §§ 1806(f), 1825(d), and 1881e apply only if the government (1) "intends to enter into evidence or otherwise use or disclose" (2) "against an aggrieved person" (3) in a "trial, hearing, or other proceeding in or before any court, department officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. §§ 1806(f), 1825(d); *see also* 50 U.S.C. § 1881e(a) (providing that information acquired pursuant to Sections 702 and 703 of FISA "shall be deemed to be information acquired pursuant to" 50 U.S.C. § 1801 *et seq.*). Where all five criteria are met, the government will notify the defendant and the Court or other authority in which the information is to be used or disclosed that the United States intends to use or disclose such information. The government has complied with those provisions in this case. On April 8, 2016, the government provided the defendant with notice pursuant to 50 U.S.C. §§ 1825(d) and 1881e(a) that it intended to use evidence "obtained or derived from physical searches and acquisitions" conducted pursuant to FISA against the defendant at trial. (Doc. 14). The government's notice gave the defendant all the information to which he was entitled and that was necessary to file a motion to suppress.

In the context of FISA collection, Congress has made a decision to allow for greater protection of information than is normally afforded because of the need to protect sensitive national security information, which includes classified sources and methods. Congress intended that FISA “reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.” S. Rep. No. 95-701 at 16. As such, in recognition of “the nature of the national interests implicated in matters involving a foreign power or its agents,” Congress provided for more limited disclosure than is ordinarily provided with regard to criminal evidence. *Belfield*, 692 F.2d at 148.

The defendant’s position that he is entitled to more information regarding FISA-authorized collection is further refuted by the fact that Congress did provide for broader notice of FISA surveillance in certain situations, but declined to do so in the notice sections applicable to criminal defendants. *See Dean v. United States*, 556 U.S. 568, 573 (2009) (“[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”). Specifically, Congress identified three scenarios where more specific notice regarding FISA surveillance was warranted. *See* 50 U.S.C. § 1806(j) (notice of particular information regarding surveillance required where the Attorney General approves emergency surveillance and the government does not later obtain authorization from the FISC); 50 U.S.C. § 1825(b) (requiring notice identifying property seized, altered, or reproduced during physical search of a U.S. person’s residence where the Attorney

General has determined that there is no national security interest in continued secrecy); 50 U.S.C. § 1825(j) (notice of particular information regarding physical search required where the Attorney General approves emergency physical search and the government does not later obtain authorization from the FISC). Congress elected not to require such broad disclosure in the situation where a defendant is charged in a criminal proceeding. *See* 50 U.S.C. §§ 1806(c), 1825(d) (requiring only notice that “the United States intends” to use or disclose FISA-obtained or -derived information).

Nevertheless, the defendant argues that he is entitled to additional notice and discovery under 18 U.S.C. § 3504. (Doc. 51 at 12-13; Doc. 52 at 23-24). That section provides in relevant part:

In any trial, hearing, or other proceeding in or before any court . . . [u]pon 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 exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act.

However, 18 U.S.C. § 3504 is not applicable here because no “unlawful act” has occurred. 18 U.S.C. § 3504(a)(1) & (b). The FISA evidence was not the product of an unlawful act; to the contrary, it was lawfully obtained pursuant to orders of the FISC. Moreover, the government provided the notice required under the FISA statute (50 U.S.C. §§ 1806(c) and 1825(d)), which is the more specific notice provision that applies in this case. No court has held that in addition to 50 U.S.C. §§ 1806(c) or 1825(d), the government has an additional notice requirement under 18 U.S.C. § 3504. A specific statutory provision normally controls over one of more general application. *Bloate v. United States*, 559 U.S. 196, 207 (2010); *Gozlon-Peretz v. United States*, 498 U.S. 395,

407 (1991). Moreover, 50 U.S.C. §§ 1806 and 1825 were enacted in 1978, approximately seven years after 18 U.S.C. § 3504 was adopted in 1970. See Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 702, 84 Stat. 922, 935-36 (1970). “[A] later enacted statute may limit the scope of an earlier statute.” *Bhd. of Maintenance of Way Emp. v. CSX Transp., Inc.*, 478 F.3d 814, 817 (7th Cir. 2007); see also *Acosta v. Gonzales*, 439 F.3d 550, 555 (9th Cir. 2006) (“[C]onflicting statutes should be interpreted so as to give effect to each but to allow a later enacted, more specific statute to amend an earlier, more general statute.”) (citations omitted). Thus, there is no basis for holding that 18 U.S.C. § 3504 trumps FISA’s later-enacted, more specific notice provisions. Finally, the defendant has failed to establish a colorable basis to believe that he has been aggrieved by unlawful surveillance of any kind.⁹²

For the foregoing reasons, the Court should deny the defendant’s motions for notice and discovery.

⁹² Although the defendant cites *United States v. Apple* for the proposition that his showing of alleged illegal surveillance “need not be complete,” (Doc. 52 at 23), the court in *Apple* in fact stated that there must be a “colorable basis” to believe the defendant was aggrieved by the surveillance. 915 F.2d 899, 905 (4th Cir. 1990). In his argument concerning E.O. 12333, for example, the defendant makes only bare assertions, together with citations to newspaper articles about such collection, which is exactly the type of showing that courts have found insufficient to establish a colorable claim of illegality. See, e.g., *United States v. Aref*, 285 F. App’x 784, 793 (2d Cir. 2008) (summary order) (finding insufficient defendant’s showing that consisted of statements “by unnamed sources in a newspaper article”); *United States v. Londono-Cardoña*, No. 05-10304-GAO, 2008 WL 313473, at *2 (D. Mass. Feb. 1, 2008) (finding insufficient defendants’ showing of proffered Drug Enforcement Agency teletype messages that referred “only to apparently lawful surveillance in Colombia,” and a newspaper article discussing alleged warrantless domestic wiretapping that had “no relevance” to the defendants’ case); *In re Grand Jury Investigation*, 431 F. Supp. 2d 584, 591 (E.D. Va. 2006) (finding insufficient defense showing of “bare allegations that the government has been intercepting communications through illegal electronic surveillance”).

[CLASSIFIED MATERIAL REDACTED]

VIII. CONCLUSION

Based on the above discussion and analysis, the government requests that the Court deny defendant al-Jayab's Motion to Suppress Evidence Obtained or Derived from Warrantless Surveillance under Section 702 of the FISA Amendments Act, Motion for Notice of Surveillance Techniques Used During the Course of the Investigation, and Motion for Discovery Regarding the Intelligence Agencies' Surveillance Pursuant to Executive Order 12333.

Respectfully submitted this 23rd day of May, 2017.

JOEL R. LEVIN
Acting United States Attorney
Northern District of Illinois

DANA J. BOENTE
Acting Assistant Attorney General for
National Security

/s/
BARRY JONAS
Assistant United States Attorney

Andrew Sigler
Trial Attorney
Counterterrorism Section
National Security Division
Department of Justice

/s/
SHOBA PILLAY
Assistant United States Attorney

Jeremy S. Balint and Chad Davis
Attorney Advisors
Office of Intelligence
National Security Division
Department of Justice

Steven L. Lane
Attorney Advisor
Office of Law and Policy
National Security Division
Department of Justice

Attorneys for Plaintiff
UNITED STATES OF AMERICA

EXHIBIT 1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,)	
)	
Plaintiff)	No. 16 CR 181
)	
v.)	Judge Sara L. Ellis
)	
AWS MOHAMMED YOUNIS AL-JAYAB,)	
)	
Defendant)	

DECLARATION AND CLAIM OF PRIVILEGE
OF THE ATTORNEY GENERAL OF THE UNITED STATES

I, Jeff Sessions, hereby declare the following:

1. I am the Attorney General of the United States of America and head of the United States Department of Justice, an Executive Department of the United States. I have official custody of and control over the files and records of the United States Department of Justice. The matters stated herein are based on my knowledge, on consideration of information available to me in my official capacity as Attorney General, on discussions that I have had with other Justice Department officials, and on conclusions I have reached after my review of this information.

2. Under the authority of 50 U.S.C. §§ 1825(g) and 1881e(a), I submit this declaration pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, in connection with the above-captioned criminal proceeding. I have been advised that the Government presently intends to use information obtained or derived from physical searches and the targeting of non-U.S. persons outside the United States, all conducted pursuant to FISA, in the criminal proceeding against Aws Mohammed Younis al-Jayab (hereinafter, "the Defendant").

See 50 U.S.C. §§ 1825(d) and 1881e(a). Accordingly, the Defendant, by and through his attorney, has filed a motion seeking suppression of FISA-related information (hereinafter the “Defendant’s Motion”). The Government will file an opposition to the Defendant’s Motion. For the reasons set forth in the Government’s Opposition, it is necessary to provide this Court with the application(s) and certification(s) submitted to, and the orders issued by, the Foreign Intelligence Surveillance Court, as well as other related documents (hereinafter collectively referred to as “the FISA materials”).

3. Based on the facts and considerations set forth below, I hereby claim that it would harm the national security of the United States to disclose or hold an adversary hearing with respect to the FISA materials. The United States will be submitting the relevant classified documents to this Court as part of a “Sealed Appendix,” so this Court may conduct an *in camera*, *ex parte* review of the legality of the FISA collection at issue. My Claim of Privilege also extends to the classified portions of any memoranda, briefs, or other documents the Government may file in connection with this litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA materials.

4. In support of my Claim of Privilege, the United States is submitting to the Court for *in camera*, *ex parte* review the Declarations of Daniel R. Coats, Director of National Intelligence, and Bradley G. Mendenhall, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation. The Declarations of Mr. Coats and Mr. Mendenhall set forth, in detail, the specific facts on which my Claim of Privilege is based. The Declarations of Mr. Coats and Mr. Mendenhall are classified at the “TOP SECRET” level.

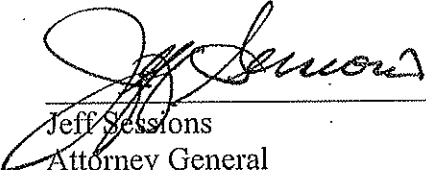
5. Relying on the facts set forth in the Declarations of Mr. Coats and Mr. Mendenhall, I certify that the unauthorized disclosure of the FISA materials that are classified at the “TOP SECRET” level reasonably could be expected to cause exceptionally grave damage to the

national security of the United States. I further certify that the unauthorized disclosure of the FISA materials that are classified at the "SECRET" level reasonably could be expected to cause serious damage to the national security of the United States. The FISA materials contain sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct counterterrorism investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of the information could harm the national security interests of the United States.

6. I respectfully request that the Court treat the contents of the Sealed Appendix, for security purposes, in the same sensitive manner that the ~~contents were treated~~ in the submission to this Court, and to return the Sealed Appendix to the Department of Justice upon the disposition of the Defendant's Motions. The Department of Justice ~~will~~ retain the Sealed Appendix under the seal of the Court subject to any further orders of this Court or other courts of competent jurisdiction.

Pursuant to Title 28, United States Code, Section 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on the 19th day of MAY, 2017.



Jeff Sessions
Attorney General