

No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

MOHAMED OSMAN MOHAMUD,

Petitioner,

v.

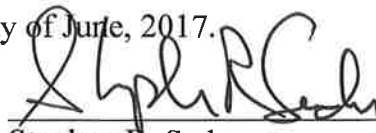
UNITED STATES OF AMERICA,

Respondent.

MOTION FOR LEAVE
TO PROCEED *IN FORMA PAUPERIS*

The petitioner, Mohamed Osman Mohamud, requests leave to file the attached petition for writ of certiorari to the United States Court of Appeals for the Ninth Circuit without prepayment of costs and to proceed *in forma pauperis* pursuant to Rule 39.1 of this Court and 18 U.S.C. § 3006A(d)(7). The petitioner was represented by counsel appointed under the Criminal Justice Act in the District of Oregon and on appeal in the Ninth Circuit Court of Appeals, and therefore no affidavit is required.

Respectfully submitted this 14th day of June, 2017.



Stephen R. Sady
Attorney for Petitioner

No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

MOHAMED OSMAN MOHAMUD,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To
The United States Court Of Appeals For The Ninth Circuit

PETITION FOR WRIT OF CERTIORARI

Stephen R. Sady
Counsel of Record
Chief Deputy Federal Public Defender
Lisa C. Hay
Federal Public Defender
Mark Ahlemeyer
Elizabeth G. Daily
Assistant Federal Public Defenders
101 SW Main Street, Suite 1700
Portland, Oregon 97204
steve_sady@fd.org
(503) 326-2123

Steven Toby Wax
Attorney at Law
630 SW 5th Avenue, Suite 500
Portland, Oregon 97204
(503) 830-7758

Attorneys for Petitioner

QUESTIONS PRESENTED

Do the Fourth Amendment and the separation of powers doctrine prohibit the government's seizure, retention, search, and subsequent use of United States citizens' emails and other private internet and telephonic communications under § 702 of the Foreign Intelligence Surveillance Act, where those searches are conducted in the United States in the absence of any judicial warrant or individualized judicial review?

Where this Court's precedent places the burden of proving harmless error on the government, should the Sixth Amendment right to jury trial and the separation of powers doctrine foreclose circuit courts from sua sponte declaring preserved trial errors to be harmless when the government has not raised harmlessness; and, if such sua sponte review is permitted, should this Court exercise its supervisory authority to articulate a clearer and fairer standard?

TABLE OF CONTENTS

	Page
Table of Authorities.....	iii
1. Opinions Below	1
2. Jurisdictional Statement.....	2
3. Constitutional And Statutory Provisions	2
4. Statement Of The Case	3
A. Summary Of The Trial Evidence	5
B. Summary Of The Entrapment Defense	8
C. Facts Related To Warrantless Surveillance And Derivative Use Of The Content Of Electronic Communications.	9
D. Facts Related To The Court Of Appeals’ Sua Sponte Determination Of Harmless Error.	13
5. Reasons For Granting The Writ.....	17
A. The Ninth Circuit’s Decision Upholding Warrantless Surveillance Under § 702 Conflicts With This Court’s Fourth Amendment Precedent And The Law Of The Sixth Circuit, And It Presents A Question Of Exceptional National Importance.	17
1. The Ninth Circuit Improperly Created A New Exception To The Warrant Requirement, Contrary To This Court’s Precedent.	19
2. The Ninth Circuit’s Conclusion That Americans Have “Diminished” Expectations Of Privacy In Their Emails Conflicts With The Sixth Circuit’s Full Protection For Private Electronic Communications.	23
3. This Court Should Grant Full Review Of § 702’s Constitutionality Because It Presents Questions Of Exceptional National Importance.	26

B.	The Judicial Rule Permitting Sua Sponte Harmless Error Review By Courts Of Appeals Violates This Court’s Precedent In A Manner That Infringes On Sixth Amendment Jury Trial Rights And The Separation Of Powers Doctrine, And, If Such A Practice Is Permissible, This Court Should Reject Its Present Formulation.	29
1.	Pursuant To A Judicial Rule Neither Promulgated By Congress Nor Approved By This Court, The Courts Of Appeals Sua Sponte Address Harmless Error In Criminal Appeals To Affirm Jury Trials Tainted By Preserved Error.	30
2.	The <i>Giovannetti</i> Rule Constitutes An Unauthorized Departure From This Court’s Precedent That Places The Burden Of Proving Harmless Error On The Government.	32
3.	If Sua Sponte Harmless Error Review Is Ever Permissible In The Direct Review Of Criminal Cases, This Court Should Reject The <i>Giovannetti</i> Rule And Articulate A Clearer Standard.	35
4.	The Present Case Provides An Ideal Vehicle For Review Of An Exceptionally Important Issue That, By Its Nature, Avoids Adversarial Appellate Review.	36
6.	Conclusion.....	40

INDEX TO APPENDIX

<i>United States v. Mohamud</i> , No. 14-30217 (9th Cir. Dec. 5, 2016) (published)	1
<i>United States v. Mohamud</i> , No. 14-30217 (9th Cir. Dec. 5, 2016) (unpublished)	51
<i>United States v. Mohamud</i> , No. 3:10-cr-00475-KI (D. Or. June 24, 2014) (unpublished)	62
Section 702 of the FISA Amendments Act	118
Chart on proliferation of the <i>Giovannetti</i> rule	129
<i>United States v. Mohamud</i> , No. 14-30217 (9th Cir. Mar. 16, 2017) (denial of rehearing and rehearing en banc)	130

TABLE OF AUTHORITIES

Page

FEDERAL CASES

<i>ACLU v. Clapper</i> , 785 F.3d 787 (2d Cir. 2015)	29
<i>Arizona v. Fulminante</i> , 499 U.S. 279 (1991)	39
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987)	23
<i>Ashcroft v. al-Kidd</i> , 563 U.S. 731 (2011)	22
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	13, 19, 25, 27
<i>Boyd v. United States</i> , 116 U.S. 616 (1886)	25
<i>Bumper v. North Carolina</i> , 391 U.S. 543 (1968)	33
<i>Caperton v. A.T. Massey Coal Co.</i> , 556 U.S. 868 (2009)	33
<i>Chapman v. California</i> , 386 U.S. 18 (1967)	29, 33, 36
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000)	22
<i>City of Los Angeles v. Patel</i> , 135 S. Ct. 2443 (2015)	27
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013)	26
<i>County of Los Angeles v. Mendez</i> , No. 16-369, 2017 WL 2322832 (U.S. May 30, 2017)	22
<i>Delaware v. Van Arsdall</i> , 475 U.S. 673 (1986)	35
<i>Fahy v. Connecticut</i> , 375 U.S. 85 (1963)	39

<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991)	23
<i>Georgia v. Randolph</i> , 547 U.S. 103 (2006)	17, 21
<i>Greenlaw v. United States</i> , 554 U.S. 237 (2008)	33
<i>Hanna v. Plumer</i> , 380 U.S. 460 (1965)	35
<i>Herring v. New York</i> , 422 U.S. 853 (1975)	34
<i>Hitchcock v. Dugger</i> , 481 U.S. 393 (1987)	33
<i>Jacobson v. United States</i> , 503 U.S. 540 (1992)	8
<i>Jones v. United States</i> , 357 U.S. 493 (1958)	17
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	17, 25
<i>Kotteakos v. United States</i> , 328 U.S. 750 (1946)	29
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	25
<i>Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach</i> , 523 U.S. 26 (1998)	35
<i>Miller v. French</i> , 530 U.S. 327 (2000)	3
<i>Mollett v. Mullin</i> , 348 F.3d 902 (10th Cir. 2003)	32
<i>In re Murchison</i> , 349 U.S. 133 (1955)	33
<i>Ocampo v. Vail</i> , 649 F.3d 1098 (9th Cir. 2011)	38-39

<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	18, 23, 25
<i>Rodriguez v. United States</i> , 135 S. Ct. 1609 (2015)	23
<i>Satterwhite v. Texas</i> , 486 U.S. 249 (1988)	36
<i>Segura v. United States</i> , 468 U.S. 796 (1984)	23
<i>Shepard v. United States</i> , 290 U.S. 96 (1933)	15
<i>Smith v. Illinois</i> , 390 U.S. 129 (1968)	40
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968)	22
<i>United States v. Adams</i> , 1 F.3d 1566 (11th Cir. 1993)	32
<i>United States v. Donovan</i> , 429 U.S. 413 (1977)	20
<i>United States v. Ford</i> , 550 F.3d 975 (10th Cir. 2008)	37
<i>United States v. Giovannetti</i> , 928 F.2d 225 (7th Cir. 1991)	29-37
<i>United States v. Gonzalez-Flores</i> , 418 F.3d 1093 (9th Cir. 2005)	17
<i>United States v. Holly</i> , 488 F.3d 1298 (10th Cir. 2007)	32
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	26
<i>United States v. Kahn</i> , 415 U.S. 143 (1974)	20
<i>United States v. Little</i> , 829 F.3d 1177 (10th Cir. 2016)	32

<i>United States v. McLaughlin</i> , 126 F.3d 130 (3d Cir. 1997)	32
<i>United States v. Mohamed Osman Mohamud</i> , 666 F. App'x 591 (9th Cir. 2016)	1
<i>United States v. Mohamud</i> , 843 F.3d 420 (9th Cir. 2016)	1, 15
<i>United States v. Montgomery</i> , 100 F.3d 1404 (8th Cir. 1996)	32
<i>United States v. Pryce</i> , 938 F.2d 1343 (D.C. Cir. 1991)	31
<i>United States v. Rodriguez-Preciado</i> , 399 F.3d 1118 (9th Cir. 2005)	32
<i>United States v. Rodriguez-Preciado</i> , 416 F.3d 939 (9th Cir. 2005)	32
<i>United States v. Rose</i> , 104 F.3d 1408 (1st Cir. 1997)	31
<i>United States v. Silva</i> , 380 F.3d 1018 (7th Cir. 2004)	39
<i>United States v. United States Dist. Ct. for the E. Dist. Of Mich.</i> , 407 U.S. 297 (1972)	<i>passim</i>
<i>United States v. Verdugo-Urquidez</i> , 494 U.S. 259 (1990)	13, 21
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	4, 18, 24
<i>Weiler v. United States</i> , 323 U.S. 606 (1945)	36
<i>Whren v. United States</i> , 517 U.S. 806 (1996)	22
<i>Wood v. Milyard</i> , 132 S. Ct. 1826 (2012)	33
FEDERAL STATUTES	
28 U.S.C. § 1254(1)	2

50 U.S.C. § 1801(e)	18
50 U.S.C. § 1806(c)	2, 12
50 U.S.C. § 1806(g)	3, 27
50 U.S.C. § 1881a	2, 12

STATE CASES

<i>State v. Almaraz</i> , 154 Idaho 584, 301 P.3d 242 (2013)	33
<i>State v. Hill</i> , 161 Idaho 444, 387 P.3d 112 (2016)	32, 33

OTHER

Orin S. Kerr, <i>Applying the Fourth Amendment to the Internet: A General Approach</i> , 62 Stan. L. Rev. 1005 (2010)	26
Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, <i>No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror</i> , 100 Minn. L. Rev. 2251 (2016)	27
Richard A. Posner, <i>Excessive Sanctions for Governmental Misconduct in Criminal Cases</i> , 57 Wash. L. Rev. 635 (1982)	35
Richard A. Posner & William M. Landes, <i>Harmless Error</i> , 30 J. Legal Stud. 161 (2001)	34
Patrick Toomey & Brett Max Kaufman, <i>The Notice Paradox: Secret Surveillance, Criminal Defendants, & The Right To Notice</i> , 54 Santa Clara L. Rev. 843 (2015)	26

No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

MOHAMED OSMAN MOHAMUD,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To
The United States Court Of Appeals For The Ninth Circuit

The petitioner, Mohamed Osman Mohamud, respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit in this case.

1. Opinions Below

The Ninth Circuit issued published and unpublished opinions reported at *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016), and *United States v. Mohamud*, 666 F. App'x 591 (9th Cir. 2016), which are reprinted in the Appendix at 1 and 51, respectively. The opinion of the District Court for the District of Oregon is reprinted in the Appendix at 62.

2. Jurisdictional Statement

The judgment of the Ninth Circuit was entered on December 5, 2016. A timely petition for rehearing or rehearing en banc was denied on March 16, 2017. App. 130. This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

3. Constitutional And Statutory Provisions

The Fourth Amendment states:

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

Section 702 of the Foreign Intelligence Surveillance Act, enacted in 2008 as part of the FISA Amendments Act, authorizes procedures for targeting persons outside the United States, other than United States persons, as a supplement to the provisions for warranted surveillance. Section 702 has been codified in 50 U.S.C. § 1881a and is attached at Appendix 118. FISA requires pretrial notice of electronic surveillance:

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, . . . of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

50 U.S.C. § 1806(c). If the district court “determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the

evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person.” 50 U.S.C. § 1806(g).

The Fifth Amendment states: “No person shall . . . be deprived of life, liberty, or property, without due process of law; . . .” The Sixth Amendment states in relevant part: “In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.” The constitutional separation of powers is expressed in the first three Articles of the Constitution. *Miller v. French*, 530 U.S. 327, 341 (2000).

Rule 2 of the Federal Rules of Criminal Procedure states: “These rules are to be interpreted to provide for the just determination of every criminal proceeding, to secure simplicity in procedure and fairness in administration, and to eliminate unjustifiable expense and delay.” Rule 52 of the Federal Rules of Criminal Procedure states: “Any error, defect, irregularity, or variance that does not affect substantial rights must be disregarded.”

4. Statement Of The Case

This case raises two recurring issues of national importance: 1) the government’s warrantless searches and use of the content of the electronic communications of millions of Americans; and 2) the courts of appeals’ deviation from this Court’s precedent by conducting sua sponte harmless error determinations that compromise judicial neutrality and jury trial rights. The case began with the warrantless electronic surveillance of an American teenager. It culminated in a fictional bomb plot designed and encouraged by the government. Based on information gleaned from warrantless searches of Mr. Mohamud’s emails, agents mounted an

aggressive and sophisticated sting operation that placed Mr. Mohamud at the center of a fake terrorist cell with plans to detonate a fake bomb in Portland's Pioneer Square. The 19-year-old defendant was the only one who did not know the whole campaign was a sham. As the Ninth Circuit recognized, Mr. Mohamud was "a teenager with no criminal record, [who] had neither the means nor the intent to commit domestic terrorism until he became involved with the undercover FBI [operatives]." App. 21. Given what it characterized as the "quite aggressive" government conduct to ensnare the defendant, the Ninth Circuit found that the three-week trial involved a "solid case" for entrapment. App. 31, 25.

The Ninth Circuit's ruling affirming the lawfulness of warrantless electronic surveillance under § 702 of the FISA Amendments Act (FAA) conflicts with this Court's precedent and with the Sixth Circuit's decision in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The question is of exceptional importance because, under § 702, the government intrudes on the electronic communication privacy of massive numbers of United States citizens by reading and listening to the content of their electronic communications without the traditional protections of individualized judicial review.

The Ninth Circuit's sua sponte ruling that declared preserved trial errors to be harmless also involves an issue of national importance. From a single per curiam decision in 1991, the courts of appeals have abandoned this Court's precedent placing the burden to prove harmlessness on the prosecution. This Court should grant review to vindicate its precedent and restore protections for judicial neutrality and the endangered right to jury trial. The historical facts of this case are largely undisputed and are summarized to provide context for the issues of law presented in this petition.

A. Summary Of The Trial Evidence

Mohamed Osman Mohamud was born in war-torn and impoverished Somalia on August 11, 1991. His father emigrated to the United States as a refugee in 1993, and his son and wife followed about a year later. Although mother and child were malnourished, the reunited family was happy to be in the United States, where Mr. Mohamud was eventually naturalized as an American citizen. From the time of his arrival in the United States until his early teen years, Mr. Mohamud was an ordinary immigrant youngster with a diverse group of friends. His family attended the local mosque, where they socialized with others in the Muslim community. During his sophomore year in high school, Mr. Mohamud won an award for a poem he wrote about the reasons he loved Oregon. Childhood friends and former teachers described Mr. Mohamud as “goofy,” “fun-loving,” “very friendly,” and “a great kid.”

As a teenager, Mr. Mohamud experienced what his father described as a normal teenage “identity crisis” about his religion and culture. Unbeknownst to his father, Mr. Mohamud began researching religion on the internet where he encountered pro-jihadi websites and became very familiar with the extremist language of that internet community. In his senior year of high school, he pseudonymously wrote four articles for an online extremist magazine called “Jihad Recollections.” On August 31, 2009, shortly after Mr. Mohamud’s eighteenth birthday, his father contacted the Federal Bureau of Investigation because he feared his son was trying to go abroad where he would be in danger. A short time later, the father advised the FBI that Mr. Mohamud did not have a ticket or visa and so was not an imminent risk to leave the country, as he had feared. Mr. Mohamud’s father learned that his son knew a person named Amro from his mosque who was helping him find a school for study in Yemen. The father’s

concern led the FBI to connect Mr. Mohamud with ongoing electronic surveillance. The FBI began all-encompassing surveillance, which followed the son as he went off to college at Oregon State University.

As the school year progressed, Mr. Mohamud became deeply involved in the college social scene, including abuse of alcohol and drugs. The case agent reported that he did not seem as involved in extremism and was a conflicted and manipulable kid. After considering various options, on November 9, 2009, an FBI operative began what would become a six-month email correspondence with Mr. Mohamud, with the operative feigning that he was “Bill Smith,” a fellow Muslim in the United States with ideas about taking “action against the West.” Mr. Mohamud responded to the email conversations but did not say anything regarding researching, planning, or intending to use weapons of mass destruction in the United States. Mr. Mohamud eventually ceased communications with the undercover operative in May 2010.

On December 3, 2009, Mr. Mohamud received an email from “Amro” regarding travel abroad. While Mr. Mohamud believed Amro was still in Yemen, the FBI traced the email to the northwest frontier region of Pakistan. Mr. Mohamud attempted unsuccessfully to respond to the email over the next several months. He also corresponded with an American friend who was studying in Saudi Arabia. The government asserted that a phrase in an email to the friend regarding martyrdom had an ominous meaning, while the defense presented evidence that it was innocuous.

On June 7, 2010, FBI agents received a “green light to target” Mr. Mohamud. On June 14, 2010, FBI agents stopped Mr. Mohamud and his family as he attempted to board an airplane to Alaska for a summer job at a cannery, informing Mr. Mohamud that he would not

be allowed to fly. During the interview with the FBI, Mr. Mohamud referred to “Amr” as the person he knew who had referred him to a school in Yemen, but stated that he did not intend to travel there presently.

On June 23, 2010, the FBI arranged to have an agent begin email contact with Mr. Mohamud as a feigned associate of Amro al-Ali. When asked whether he could “help the brothers,” Mr. Mohamud stated that he could not travel and that he would communicate if that changed. In response, the agent sent a message saying that Allah “I’m sure has good reason for you to stay where you are,” and asked for a personal meeting.

During an initial meeting that was not recorded, the undercover agent Youssef asserted that he was a representative of a religious council and that Mr. Mohamud was one of seven candidates being interviewed to determine who could help the cause. When asked what Mr. Mohamud had done to show he was a good Muslim, Mr. Mohamud responded by referring to his writing. When asked what he could do to help, Mr. Mohamud said “anything.” Then, when given options including becoming “operational,” he indicated he would do so. The agent asked Mr. Mohamud to identify a target in Portland. At the next meeting, Youssef introduced the second undercover operative, Hussein, who pretended to be the explosives expert needed to approve the plan. Mr. Mohamud identified the target as Portland’s Pioneer Square during the Christmas tree lighting ceremony on the Friday after Thanksgiving.

As reflected in numerous recorded phone calls and meetings, Mr. Mohamud carried out instructions from the undercover operatives and expressed enthusiasm for the plan over the next four months. He purchased purported bomb parts, rented a storage locker, scouted locations, participated in a mock test explosion, and prepared a video in which he explained

the justification for action against the United States. On the date planned, Hussein handed Mr. Mohamud a cell phone, and Mr. Mohamud pressed the buttons that he believed would set off a massive explosion during festivities with thousands present. When nothing happened, Mr. Mohamud pressed the buttons a second time on the instruction of Hussein, then was arrested.

B. Summary Of The Entrapment Defense

The entrapment theory of defense followed this Court's holding in *Jacobsen v. United States*, 503 U.S. 540, 548-52 & n.3 (1992), by requiring the government to prove beyond a reasonable doubt that Mr. Mohamud was predisposed at the time of the first government contact to commit the specific crime charged in the indictment, which was attempted use of a weapon of mass destruction in the United States. In favor of the defense: the exhaustive surveillance and collateral investigations revealed no evidence that Mr. Mohamud had researched, planned, or intended to carry out a domestic attack prior to the beginning of government contact, and, at the time of first contact, the FBI case agent characterized him as "conflicted" and "manipulable." In favor of the government: as a 17-year-old high school senior, Mr. Mohamud expressed resentments against American actions abroad and solidarity with extremists including Osama bin Laden, wrote for blogs and an extremist electronic magazine, expressed interest in going overseas, and, during meetings with undercover agents, made extreme and inflammatory statements regarding terrorism.

The defense presented evidence through family, friends, and others that Mr. Mohamud was an ordinary child growing up without indications of violence. Schoolmates testified about good works and ordinary activities in high school and college. The defense called three experts in support of acquittal: an expert in adolescent psychology; an expert in the social psychology

of context in reinforcing deviate behaviors; and a counter-terrorism psychiatric expert who opined that, when the government contacts began, Mr. Mohamud was a talker, but did not pose a genuine threat of violence.

After closing arguments, the jury sent a note asking the court to clarify the correct standard for predisposition in relation to the crime charged (“Where [the jury instruction] states ‘the crime,’ does that refer strictly to the crime as stated in the indictment, or could it include ‘a similar’ crime as stated by the prosecutor in closing statement?”). The court refused to provide the answer requested by the defense (“‘commit the crime’ refers to the crime set forth in the indictment”), and, instead, instructed over objection, “The jury may consider evidence of similar conduct or willingness to engage in similar conduct, along with all the evidence, in deciding if the defendant was predisposed to commit the crime set forth in the indictment.” The jury returned a verdict of guilty shortly thereafter.

At sentencing, the defense asserted that a mitigated sentence was warranted based on imperfect entrapment, Mr. Mohamud’s pretrial cooperation with the government, and evidence of his extraordinary rehabilitation, including repeated renunciations of violence. Two highly qualified psychiatrists provided uncontroverted reports that Mr. Mohamud presented a very low risk of future dangerousness. The trial judge sentenced Mr. Mohamud to 30 years in prison.

C. Facts Related To Warrantless Surveillance And Derivative Use Of The Content Of Electronic Communications.

Section 702 of the FAA expanded the executive branch’s ability to seize and search the contents of American citizens’ communications under FISA. In *United States v. United States*

Dist. Ct. for the E. Dist. Of Mich., this Court required full compliance with the warrant requirement for domestic national security eavesdropping, while implicitly suggesting that a framework for surveillance of foreign powers would be constitutionally permissible. 407 U.S. 297, 322-23 (1972) (*Keith*). In response to executive branch overreach, Congress enacted FISA in 1978, which established a Foreign Intelligence Surveillance Court and authorized the issuance of individualized warrants, supported by probable cause, for the electronic surveillance of foreign powers and their agents at specific facilities and places. FISA required the government to use “minimization procedures” designed to minimize the acquisition and retention, and prohibit the dissemination, of private information acquired about Americans through the surveillance. The courts of appeals have generally upheld FISA warrants under the Fourth Amendment.

The FISA Amendments Act of 2008 radically changed the FISA structure. Under § 702, when the government claims to be “targeting” aliens abroad, it no longer need comply with FISA’s requirements of 1) individualized court orders 2) based on a determination of probable cause 3) particularly describing the place or facility monitored 4) with limitations on the time of surveillance. Instead, § 702 created an administrative system in which intelligence agencies unilaterally select and approve targets of surveillance. The FISC reviews and approves the agencies’ general “targeting” and “minimization” protocols once a year, and does not review individual instances of surveillance. This framework results in the surveillance of tens of thousands of foreign targets annually and the “incidental” collection of millions of communications belonging to United States citizens.

The targeting and minimization procedures allow the government wide latitude to seize, retain, and use the content of Americans' communications without a warrant. The government's overseas targets need not be foreign agents, terrorists, or suspected of any wrongdoing whatsoever; instead, the target may be anyone the government believes is likely to communicate "foreign intelligence information." When this warrantless surveillance results in the collection of Americans' communications – as it often does – the protocols permit the government to keep those communications for years. Once collected, the protocols allow the American communications to be retained, searched, and used for both foreign intelligence and criminal purposes. The government has asserted that it can freely examine and use the content of American communications once they have been lawfully collected.

One of the principal ways in which the government uses the collection of retained Americans' communications is through so-called "secondary searches." The government aggregates the millions of communications it collects in intelligence databases and then searches through those databases for the communications of specific Americans, without ever obtaining judicial approval. In this way, agents are able to access the contents of private communications that they would otherwise be prohibited from accessing without a warrant. Official government disclosures indicate that FBI agents perform such secondary searches in virtually every national security investigation, presumably including the FBI's investigation of Mr. Mohamud. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, at 59 (July 2, 2014).

In the 26 months prior to the trial in January 2013, the defense moved for discovery of all warrantless surveillance of Mr. Mohamud, with specific requests for warrantless surveillance from which other evidence was derived. The government repeatedly asserted that it had complied with all discovery obligations. On November 9, 2013, ten months *after* the trial, the government filed a supplemental notice stating that “pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), [] the government has offered into evidence or otherwise used or disclosed in proceedings, including at trial, in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.” District Court Docket 486. In other words, the government acknowledged that Mr. Mohamud had been subjected to warrantless surveillance under § 702, and the government used information derived from that surveillance in proceedings against him, including at trial.

The defense responded to the disclosure with motions for discovery regarding the surveillance, for dismissal or suppression based on the failure to provide pretrial notice as required by statute, and for suppression because the warrantless surveillance and searches of the content of Americans’ electronic communications was not authorized by the statute and violated the Fourth Amendment. The district court denied all motions. The district court wrote that the lawfulness of a secondary search of incidentally seized American communications presented a “very close question” and was the “most persuasive argument.” App. 103, 106. However, the court ultimately concluded that the search was reasonable under the foreign intelligence exception to the Fourth Amendment’s warrant requirement.

The Ninth Circuit affirmed on different grounds. App. 43 n.25 (“Because the incidental collection excepts this search from the Fourth Amendment’s warrant requirement, we need not address any ‘foreign intelligence exception.’”). First, the court relied on *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), to hold that the surveillance was exempted from the Fourth Amendment’s warrant requirement because the government subjectively intended to “target” only individuals with no Fourth Amendment rights – aliens communicating abroad – even though the government anticipated that it would incidentally collect millions of Americans’ communications as well. Second, the court held that the surveillance was “reasonable” because Americans have reduced privacy interests in emails once sent to the receiving party. In support of this “reasonableness” rationale, the court stated that it did not have to address the secondary search issue pointedly raised in the district court’s decision because, in the panel’s opinion, the case did not involve “retention and querying” of seized American communications. App. 37. The Ninth Circuit’s opinion never mentioned the two electronic surveillance cases upon which the defense placed primary reliance: *Keith* and *Berger v. New York*, 388 U.S. 41 (1967).

D. Facts Related To The Court Of Appeals’ Sua Sponte Determination Of Harmless Error.

In the court of appeals, the defense identified numerous, well-preserved trial errors related to the trial judge’s apparent confusion regarding “state of mind” evidence including:

- The district court allowed numerous agents to testify about an Interpol Red Notice purporting to identify Amro Al-Ali as a terrorist recruiter to establish the “course of investigation,” then permitted the government to admit the document itself into evidence. The Ninth Circuit held that the existence of the Notice was relevant as to the state of mind only of those agents who directed the investigation against Mr. Mohamud, but agreed

that “the comparable testimony of the undercover agents was not relevant, nor was the Red Notice itself,” and that the government had used the Notice for its truth in several instances.

- The district court excluded inadvertently recorded statements made by the undercover agents during the investigation that were relevant to establish bias (such as statements about what “might be a problem in front of the jury” and “whether Washington was going to consider this operation sexy enough”), and restricted use of the statements to cross-examination, which precluded the jury from assessing nuances apparent from the recordings.
- The district court excluded statements made by Mr. Mohamud before any FBI contact that were admissible as statements of his then-existing state of mind to prove his lack of predisposition.
- The district court permitted the undercover agents to provide commentary regarding what Mr. Mohamud “meant” or was “thinking” during his recorded statements (what Mr. Mohamud wanted, why he was crying, whether he was serious).

See App. 55-57. Two examples of this last type of error illustrate the district court’s misunderstanding of “state of mind” evidence. When the prosecutor asked what Mr. Mohamud meant in a recorded statement when he said that his parents did not believe in what he was doing (“what did you think he meant by that?”), the defense objected and was overruled, which led to the following:

THE WITNESS: He wanted to commit a terrorist act. He wanted to place a device at Pioneer Square.

[DEFENSE COUNSEL]: Your Honor, I’ll object and ask that that be stricken.

THE COURT: Overruled. He’s asking for his state of mind. He’s giving his state of mind. Go ahead.

In another example, the court overruled an objection to an undercover agent's testimony in response to "what did you believe he meant by 'jihad' in that context?" where the context was a pre-FBI contact conversation with a friend:

THE COURT: I'll allow it for his state of mind, the witness's state of mind, at the time.

THE WITNESS: To me, that's where individually he was trying – he was talking, the defendant, to let him go to Somalia to commit to join the As Sahab organization, which is a terrorist organization. That's what I got from the conversation; that it was helping him to do something like that.

The defense argued on appeal that this Court's precedent required reversal based on improper admission of state of mind testimony under *Shepard v. United States*, 290 U.S. 96, 104 (1933).

The government's response brief argued that the trial court committed no trial errors. The only mention of harmlessness related to the exclusion of the defendant's contemporaneous communications. As to those statements, the government asserted that "the exclusion of the few items defendant identifies was harmless" because other statements were admitted. Response Brief, Ninth Circuit Docket 53-1, at 84. The defense pointed out in the reply brief that the government did not assume its burden of proving harmlessness. Reply Brief, Ninth Circuit Docket 72, at 2.

During oral argument, one Ninth Circuit judge pointed out the government's failure to raise harmlessness as to most of the trial errors. Oral Argument at 32:16, *Mohamud*, 843 F.3d 420 (No. 14-30217) (https://www.youtube.com/watch?v=jaXQ_K3wzpg). The judge asked the government to confirm whether it was arguing that the agents' "color commentary" during the recordings of Mr. Mohamud was harmless, to which the prosecutor replied: "We did not

argue harmlessness,” then argued that the ruling was within the trial judge’s discretion. *Id.* at 31:45. Another judge clarified:

JUDGE: You’re not arguing that the rulings were erroneous but harmless. You’re arguing that the rulings were not erroneous, they were correct. Period.

PROSECUTOR: Right and well more specifically that the rulings were not an abuse of the trial judge’s discretion.

Id. at 34:40.

A judge later pointed to the line of cases allowing the court to address harmlessness when the government does not raise the issue. *Id.* at 36:00. The prosecutor again asserted that no error had occurred but agreed that the court could rely on those cases “to determine this was in fact harmless as a matter of law if it was error at all.” *Id.* at 37:40. In rebuttal, defense counsel argued that the evidence was “completely inadmissible, it’s completely harmful.” *Id.* at 1:00:30.

In its decision, the Ninth Circuit found trial error in at least three categories: the Interpol notice, the “color commentary,” and the exclusion of Mr. Mohamud’s contemporaneous communications. App. 55-59. The court also found that “the government failed to argue that the evidentiary errors were harmless,” except as to some contemporaneous statements. App. 58. Despite recognizing the multiple preserved errors and the government’s failure to argue harmlessness, the court invoked Ninth Circuit precedent that adopted the Seventh Circuit’s rule on sua sponte consideration of harmless error in “extraordinary cases.” App. 59. In a conclusory sentence without preceding or subsequent explanation, the court held that any evidentiary errors were cumulatively harmless: “Here, in the context of the entire trial record, ‘the harmlessness of the error[s] is not reasonably debatable,’ and further litigation would be

futile.” App. 59 (quoting *United States v. Gonzalez-Flores*, 418 F.3d 1093, 1101 (9th Cir. 2005)).

5. Reasons For Granting The Writ

A. The Ninth Circuit’s Decision Upholding Warrantless Surveillance Under § 702 Conflicts With This Court’s Fourth Amendment Precedent And The Law Of The Sixth Circuit, And It Presents A Question Of Exceptional National Importance.

This case squarely presents a question of extraordinary importance to the privacy rights of United States citizens in their electronic communications: whether the executive branch can retain, examine, and use their private communications collected under § 702 without first seeking any kind of individualized judicial review. This Court’s review is necessary because the Ninth Circuit’s opinion contravenes this Court’s governing Fourth Amendment precedent and creates an inter-Circuit conflict.

First, by creating a new exception to the warrant requirement based on law enforcement’s subjective intent to “target” individuals who lack Fourth Amendment protections, the Ninth Circuit’s holding conflicts with this Court’s precedent protecting United States persons’ privacy. As this Court has repeatedly held, under the Fourth Amendment, warrantless searches are per se unreasonable, subject to very few, carefully delineated exceptions. *See, e.g., Keith*, 407 U.S. at 318 (citing *Katz v. United States*, 389 U.S. 347, 357 (1967)); *Georgia v. Randolph*, 547 U.S. 103, 109 (2006) (exceptions to the warrant requirement are “jealously and carefully drawn”) (quoting *Jones v. United States*, 357 U.S. 493, 499 (1958)). Second, by claiming American citizens have “diminished” rights to privacy with respect to their personal email communications, the Ninth Circuit promulgated a rule in

conflict with the Sixth Circuit’s full protection for private emails in *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and inconsistent with this Court’s approach to the protection of electronic privacy in cases such as *Riley v. California*, 134 S. Ct. 2473, 2485 (2014) (warrant required to search the data on lawfully seized cell phones). Certiorari should be granted to resolve the conflict and bring the Ninth Circuit’s decision into conformance with this Court’s precedent.

Certiorari should also be granted because of the exceptional importance of reviewing the government’s practices under § 702. “Few threats to liberty exist which are greater than that posed by use of eavesdropping devices.” *Berger*, 388 U.S. at 63. Section 702’s lack of protections for the communications of Americans who correspond with persons abroad affects the privacy of millions of citizens. Section 702 explicitly disconnects its scope from national security by authorizing collection based on “foreign intelligence information,” which is defined so broadly that it encompasses national security and anything necessary to “the conduct of the foreign affairs of the United States.” 50 U.S.C. § 1801(e). With § 702 extending far beyond national security, intelligence agencies are free to retain and access a massive trove of private communications of United States citizens – including politicians, journalists, lawyers, judges, and members of Congress – with no check from the judiciary. The government’s implementation of § 702 risks many of the types of executive branch abuses that led to the enactment of FISA to govern foreign intelligence surveillance. Yet the Ninth Circuit – relying on reasoning in conflict with this Court’s and the Sixth Circuit’s precedents – failed to properly analyze the constitutional implications of the government’s actions.

1. *The Ninth Circuit Improperly Created A New Exception To The Warrant Requirement, Contrary To This Court's Precedent.*

The Ninth Circuit's decision conflicts with this Court's precedent because the lower court invented a broad exception to the warrant requirement for searches and seizures conducted within the United States that depends on the subjective intent of investigators to target noncitizens abroad. As this Court has held, Americans' private communications are subject to full Fourth Amendment protection from the government's electronic surveillance, and warrantless searches are per se unreasonable, subject only to narrow exceptions. *Keith*, 407 U.S. at 323-24. In *Keith*, this Court held that domestic national security surveillance is not exempt from the Fourth Amendment's warrant requirement, as informed in the national security context by the First Amendment and the separation of powers doctrine. 407 U.S. at 312-22. Similarly in *Berger*, the Court held that "the language of New York's statute [authorizing warrantless electronic surveillance] is too broad in its sweep resulting in a trespassory intrusion into a constitutionally protected area and is therefore, violative of the Fourth and Fourteenth Amendments." 388 U.S. at 44. Mr. Mohamud is a United States citizen, and the § 702 surveillance that resulted in the acquisition of his communications, and all later accessing and use of those communications, occurred within the United States. The surveillance of Mr. Mohamud's communications falls fully within the scope of *Keith* and *Berger*'s reasoning.

Although the Ninth Circuit relied on the "incidental overhear" rule as a basis for its holding that this warrantless surveillance is constitutional, the formative Supreme Court case establishing the rule involved a court-issued warrant – a factor central to its reasoning. *United*

States v. Kahn, 415 U.S. 143, 154-55 (1974) (describing the judicial determinations and limitations that foreclosed characterization of the wiretap as a general warrant). Because it is based on a finding of probable cause and drawn with particularity, a warrant authorizing the search and seizure of specific communications satisfies the Fourth Amendment rights of all parties to the communications at issue, including parties who are incidentally overheard. *See United States v. Donovan*, 429 U.S. 413, 436 n.24 (1977) (while a warrant is not made unconstitutional by “failure to identify every individual who could be expected to be overheard,” the “complete absence of prior judicial authorization would make an intercept unlawful”). The logic of the incidental overhear rule depends on the fact that a neutral judicial officer has made all the findings required to lawfully invade the privacy of the individuals whose communications will be intercepted, whether they are the government’s ostensible targets or not. Elizabeth Goitein, *The Ninth Circuit’s Constitutional Detour in Mohamud*, Just Security (Dec. 8, 2016).¹ As this Court’s cases demonstrate, the incidental overhear rule is not an “exception” to the warrant requirement, but instead flows from the existence of a valid warrant.

Thus, the reasoning of the incidental overhear cases cannot be superimposed onto § 702 searches, where no individualized judicial review ever occurs. The government has asserted that, once acquired en masse, the millions of incidentally collected communications of United States citizens have lost all constitutional privacy protections. *Public Hearing Regarding the*

¹ Available at <https://www.justsecurity.org/35411/ninth-circuits-constitutional-detour-mohamud/>

Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act Before The PCLOB, at 28 (Mar. 19, 2014) (“Once you’ve lawfully collected that information, subsequently querying that information isn’t a search under the Fourth Amendment, it’s information already in the government’s custody.”) (testimony of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice).² As the Ninth Circuit recognized, the “vast” quantity of communications expected to accompany § 702 surveillance distinguishes the program from any other type of incidental collection. App. 41. Retention and accessing of incidentally collected communications on this scale does not come close to meeting this Court’s standard that warrant exceptions be “few in number,” *Keith*, 407 U.S. at 318, and “jealously and carefully drawn.” *Randolph*, 547 U.S. at 109.

The Ninth Circuit also erred in relying on *Verdugo-Urquidez* to preempt *Keith*’s reasoning. In *Verdugo-Urquidez*, the Court addressed a search conducted in Mexico of the property of a Mexican citizen and concluded that the search was not subject to the Fourth Amendment. Here, the electronic surveillance was conducted within the United States and involved the retention and accessing of private communications of an American citizen. The critical factor in *Verdugo-Urquidez* was the extraterritorial nature of the search. 494 U.S. at 274-75 (“At the time of the search, he was a citizen and resident of Mexico with no voluntary attachment to the United States, *and the place searched was located in Mexico*. Under these

² Available at http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

circumstances, the Fourth Amendment has no application.”) (emphasis added). As reflected in Justice Kennedy’s concurrence, *Verdugo-Urquidez*’s holding was limited to “extraterritorial application of the Constitution” against a non-citizen in a place where the Fourth Amendment could not be enforced. *Id.* at 275. By contrast, there is “little doubt that full protections of the Fourth Amendment would apply” if the search had occurred within the United States. *Id.* at 278 (Kennedy, J., concurring).

The Ninth Circuit’s creation of a new warrant exception that allows agents within the United States to retain and search Americans’ communications based on the agents’ subjective intent to “target” foreign citizens abroad cannot be sustained under *Keith*, *Berger*, and *Verdugo-Urquidez*. This new exception, if left to stand, would be broad, vague, and subject to abuse. Moreover, this Court’s jurisprudence provides no basis for defining a warrant exception based on the subjective intent of the searching officer. *Ashcroft v. al-Kidd*, 563 U.S. 731, 736 (2011) (“Fourth Amendment reasonableness ‘is predominantly an objective inquiry.’”) (quoting *Indianapolis v. Edmond*, 531 U.S. 32, 47 (2000)); see *County of Los Angeles v. Mendez*, No. 16-369, 2017 WL 2322832, *7 (U.S. May 30, 2017) (“the reasonableness of a search or seizure is almost always based on objective factors”) (citing *Whren v. United States*, 517 U.S. 806, 814 (1996)). National security investigations are particularly ill-suited for an intent-based warrant exception given that secrecy insulates the agents’ claimed intent from any meaningful defense challenge.

The Ninth Circuit’s analysis also fails to meet this Court’s standard rule for Fourth Amendment scrutiny, which requires independent justification for each incremental government intrusion into a protected zone. *Terry v. Ohio*, 392 U.S. 1, 19 (1968) (the scope of

the search must be strictly tied to and justified by the circumstances that rendered its initiation permissible). The government's subjective intent to conduct a dragnet collection of communications involving foreign persons abroad provides no independent justification for warrantless searches of the contents of American communications that are seized incidentally. *See Segura v. United States*, 468 U.S. 796, 812 (1984) (a seizure reasonable at its inception may become unreasonable). Before government agents affirmatively retain, search, and use the protected communications of Americans incidentally swept up in § 702 surveillance, they must independently justify those intrusions under ordinary Fourth Amendment standards. *See Rodriguez v. United States*, 135 S. Ct. 1609, 1614-15 (2015) (prolongation of detention after purpose completed required independent Fourth Amendment justification); *Riley*, 134 S. Ct. at 2494-95 (unconstitutional to search without a warrant contents of lawfully seized cell phones); *Florida v. Jimeno*, 500 U.S. 248, 251 (1991) (warrantless search must be limited to scope of consent); *Arizona v. Hicks*, 480 U.S. 321, 326-27 (1987) (unconstitutional to move items during lawful protective sweep).

2. *The Ninth Circuit's Conclusion That Americans Have "Diminished" Expectations Of Privacy In Their Emails Conflicts With The Sixth Circuit's Full Protection For Private Electronic Communications.*

The Ninth Circuit found the surveillance in this case lawful only after concluding that Americans' expectation of privacy in their private electronic communications is "diminished" the moment those communications are sent to the recipient. App. 45. In reaching this conclusion, the court claimed that it was applying the third-party doctrine: "the communications at issue here had been sent to a third party, which reduces Mohamud's privacy

interest at least somewhat.” App. 46. The court stated, “Under the third-party doctrine, Mohamud had a reduced expectation of privacy in his communications to third parties.” App. 3. But the Ninth Circuit distorted third-party doctrine by applying it to all private communications between sender and recipient. Because communications by definition involve at least two parties, the Ninth Circuit’s logic reduces the expectation of privacy in virtually every electronic communication.

The Ninth Circuit’s erroneous reasoning conflicts with Sixth Circuit precedent holding that individuals “enjoy[] a reasonable expectation of privacy in the contents of emails ‘that are stored with, or sent or received through, a commercial [internet service provider].’” *Warshak*, 631 F.3d at 288 (citation omitted). In *Warshak*, the government subpoenaed emails from a third party service provider without judicial oversight. In its Fourth Amendment analysis, the Sixth Circuit determined that users of electronic services have a reasonable expectation that providers would not hand over the content of their emails to the government without judicial process. *Id.* at 287-88. The Sixth Circuit recognized that the “sensitive and intimate” nature of email communications warrant full Fourth Amendment privacy protections:

Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, “account” is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner’s life. By obtaining access to someone’s email, government agents gain the ability to peer deeply into his activities.

Id. at 284. The Sixth Circuit held that “government agents violated the Fourth Amendment when they obtained the contents of Warshak’s emails” and, to the extent the Stored Communications Act permitted the government to obtain such emails without a warrant, the statute was unconstitutional. *Id.* at 288.

The Ninth Circuit’s contrary conclusion that individuals have a diminished expectation of privacy in personal electronic communications they share with others is inconsistent with *Warshak* as well as with this Court’s precedent. “[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.” *Keith*, 407 U.S. at 313; *see Berger*, 388 U.S. at 63 (electronic surveillance requires compliance with the “basic command of the Fourth Amendment before the innermost secrets of one’s home or office are invaded”). This Court found that cell phones, which commonly include email capacity, are not just another technological convenience: “With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life[.]’” *Riley*, 134 S. Ct. at 2494-95 (quoting *Boyd v. United States*, 116 U.S. 616, 625 (1886)).

The Sixth Circuit’s approach, and not the Ninth Circuit’s, corresponds with the manner in which this Court has previously assessed the privacy implications of technological developments. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (evolving technology must not be permitted to “erode the privacy guaranteed by the Fourth Amendment”); *Katz*, 389 U.S. at 352 (recognizing “the vital role that the public telephone has come to play in private communication”). By taking an approach inconsistent with the Sixth Circuit, the Ninth Circuit also ignored academic analysis that the content of emails are entitled to full Fourth Amendment

protections. Compare Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1040-43 (2010), with Orin S. Kerr, *The Surprisingly Weak Reasoning of Mohamud*, Lawfare (Dec. 23, 2016).³ The contents of emails are often personal and intimate. Even beyond contents, more external information, such as the identities and locations of correspondents and the frequency of communications, can implicate privacy interests. See generally *United States v. Jones*, 565 U.S. 400, 413 (2012) (Sotomayor, J., concurring) (“[The third party doctrine] is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”). The Ninth Circuit’s holding that, merely by sending electronic communications, the expectation of privacy in communications diminishes to a constitutionally significant degree conflicts with the Sixth Circuit’s holding in *Warshak* and is inconsistent with this Court’s jurisprudence regarding technology and privacy.

3. *This Court Should Grant Full Review Of § 702’s Constitutionality Because It Presents Questions Of Exceptional National Importance.*

For almost a decade, the government has engaged in ongoing warrantless surveillance of millions of Americans that has evaded constitutional review. See *Clapper v. Amnesty International*, 133 S. Ct. 1138, 1155 (2013) (plaintiffs lacked standing to challenge § 702 surveillance); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & The Right To Notice*, 54 Santa Clara L. Rev. 843, 866-72 (2015) (describing the history of governmental non-compliance with the statutory notice

³ Available at <https://lawfareblog.com/surprisingly-weak-reasoning-mohamud>

requirement for § 702-derived evidence). Section 702's unprecedented bulk adjudication of surveillance – abandoning individualized review and authorization of particular searches by the FISC – has been called constitutionally “very questionable” on separation of powers grounds by one of FISA's authors. Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 Minn. L. Rev. 2251, 2275-79 (2016). Yet the Ninth Circuit, in contrast to this Court's detailed analyses in *Keith* and *Berger*, rejected the challenges to § 702 without conducting review commensurate with the importance of the subject.

The Ninth Circuit misapplied this Court's precedent regarding the scope of a constitutional challenge to a surveillance statute. Under *City of Los Angeles v. Patel*, “the proper focus of the constitutional inquiry is searches that the law actually authorizes, not those for which it is irrelevant.” 135 S. Ct. 2443, 2451 (2015). It is irrelevant whether § 702 constitutionally permits surveillance of a foreigner conducted overseas. Section 702 is invalid as to the content of American citizens' communications because its “blanket grant of permission to eavesdrop [on protected communications] is without adequate judicial supervision or protective procedures.” *Berger*, 388 U.S. at 60, *see Keith*, 407 U.S. at 321. Accordingly, all surveillance of the content of American communications conducted under the authority of that statute is unlawful. *See* 50 U.S.C. § 1806(g) (evidence derived from surveillance “not lawfully authorized or conducted” “shall” be suppressed).

The Ninth Circuit also improperly assessed the scope of the surveillance at issue in this case. The Ninth Circuit acknowledged the importance of minimization procedures, but did not engage in any meaningful analysis of how those procedures impact the constitutionality of

§ 702 surveillance. To the contrary, the Ninth Circuit concluded that retention and search of emails acquired pursuant to § 702 was “outside the scope of our review, as no such retention and querying is at issue in this case.” App. 44.⁴ But the degree to which minimization procedures protect Americans’ incidentally collected private communications from government intrusion is precisely at issue. The government necessarily accessed the content of an American’s incidentally collected email when it used that content to make a criminal case against him. The Ninth Circuit’s approval of a warrant exception for surveillance that “targets” foreign nationals overseas intruded on Mr. Mohamud’s privacy and constitutes a wide-open backdoor for the government to amass Americans’ personal emails and search content for law enforcement use.

Further, the Ninth Circuit’s analysis improperly adopted a piecemeal approach to the Fourth Amendment, First Amendment, and separation of powers. Those constitutional doctrines are inextricably interrelated. *Keith*, 407 U.S. at 313-14 (“National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of ‘ordinary’ crime.”); *id.* at 317 (“This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government.”). A

⁴ This contention clashes with the government’s belated notice and the premise of the district court proceedings, which involved extensive litigation of whether, once seized under § 702, the Fourth Amendment limited the government’s authority to further access and query American communications. Because the defense was denied virtually all § 702 discovery, the petitioner is unable to address the inconsistency between the premises of the Ninth Circuit’s decision and those of the district court’s opinion.

multifaceted constitutional analysis would have supported narrowly construing § 702 to prohibit use of incidentally collected American communications absent prior judicial review. *See ACLU v. Clapper*, 785 F.3d 787, 813-16 (2d Cir. 2015) (narrowly construing § 215 of the Patriot Act to prohibit the bulk collection of electronic metadata).

B. The Judicial Rule Permitting Sua Sponte Harmless Error Review By Courts Of Appeals Violates This Court's Precedent In A Manner That Infringes On Sixth Amendment Jury Trial Rights And The Separation Of Powers Doctrine, And, If Such A Practice Is Permissible, This Court Should Reject Its Present Formulation.

This Court has provided courts of appeals with the standard for determining whether preserved constitutional or non-constitutional trial errors warrant reversal. *Chapman v. California*, 386 U.S. 18, 23-24 (1967) (the prosecution must establish beyond a reasonable doubt that constitutional error did not contribute to the conviction); *Kotteakos v. United States*, 328 U.S. 750, 761-62 (1946) (the prosecution bears the burden of establishing that error did not affect substantial rights). This Court's standard places the burden of proving harmlessness on the government. When the government has not argued that a trial error is harmless, there is nothing in this Court's jurisprudence that permits the courts of appeals to affirm a conviction on harmlessness grounds. Doing so infringes on the role of judges as neutral arbiters of issues presented by the parties and encroaches on the jury's role as the sole finder of guilt or innocence.

The lower court's sua sponte consideration of harmlessness is a deviation from *Chapman* and *Kotteakos* that traces back to a single per curiam decision from the Seventh Circuit Court of Appeals: *United States v. Giovannetti*, 928 F.2d 225, 226-27 (7th Cir. 1996) (Posner, Manion, Ripple, JJ.). The disarray among the lower courts in implementing the

Giovannetti rule warrants this Court's exercise of supervisory power over rule-making and protection of the constitutional rights compromised by the rule. This Court should declare that the government fails to meet its burden to prove harmlessness by not briefing the issue. In the alternative, if some form of sua sponte review is deemed appropriate, the Court should reject *Giovannetti* and articulate a rule that better adheres to the *Chapman* and *Kotteakos* standards.

1. *Pursuant To A Judicial Rule Neither Promulgated By Congress Nor Approved By This Court, The Courts Of Appeals Sua Sponte Address Harmless Error In Criminal Appeals To Affirm Jury Trials Tainted By Preserved Error.*

Starting in 1991, the courts of appeals began departing from the standard rule requiring the government on appeal to affirmatively raise harmlessness as a defense to preserved trial errors. A per curiam panel of the Seventh Circuit read Rule 2 of the Federal Rules of Criminal Procedure to authorize courts of appeals to sua sponte declare errors harmless, even where the government has waived any claim of harmless. *Giovannetti*, 928 F.2d at 226-27. The court structured a rule based on the economic considerations of "third party interests" in efficiency:

The considerations set forth in Rule 2 help us to see that while we are not required to scour a lengthy record on our own, with no guidance from the parties, for indications of harmlessness, we are authorized, *for the sake of protecting third-party interests* including such systemic interests as the avoidance of unnecessary court delay, to disregard a harmless error even though through some regrettable oversight harmlessness is not argued to us.

Id. at 226 (emphasis added). The Court then articulated its three-part test: "[I]n deciding whether to exercise th[e] discretion [to sua sponte decide harmlessness,] the controlling considerations are [1] the length and complexity of the record, [2] whether the harmlessness of the error or errors found is certain or debatable, and [3] whether a reversal will result in protracted, costly, and ultimately futile proceedings in the district court." *Id.* at 227.

Over the years since *Giovannetti*, most Circuits and several states have adopted the Seventh Circuit’s conclusion that appellate courts may address harmlessness despite the government’s waiver of the issue by failing to brief it, but have varied in their articulation of *Giovannetti*’s three-part test for sua sponte review. The proliferation of the *Giovannetti* rule is illustrated at App. 129, which shows how the initial decision has been relied on by the Circuits, either directly or through another Circuit’s decision that depended on *Giovannetti*. The potential defects in the *Giovannetti* rule were set out in a dissent to its adoption in the District of Columbia Circuit:

- Sua sponte review conflicts with Supreme Court precedent establishing “that the government bears the burden of demonstrating on appeal that an error was harmless” and that “adversarial norms govern appellate consideration of harmless error”;
- The adversarial system relies on the “judiciary’s neutrality” and appellate courts “ordinarily have no right to consider issues not raised by a party in either briefing or argument, both because our system assumes and depends upon the assistance of counsel, []and because of the unfairness of such a practice to the other party”;
- The government’s choice not to raise harmless error in its briefing may well be telling because, “after all, the government might honestly believe that if the trial judge’s conduct was erroneous, the error had an impact on the trial.”

United States v. Pryce, 938 F.2d 1343, 1352-55 (D.C. Cir. 1991) (Silberman, J., dissenting).

Over these objections, the general outline of the *Giovannetti* three-part test has been adopted in other Circuits, but its vague terms have left the courts of appeals in disarray regarding its implementation. For example, the First Circuit expressly does not limit itself to the *Giovannetti* factors, noting the need to balance “many elements” (*United States v. Rose*, 104 F.3d 1408, 1415 (1st Cir. 1997)), while the Tenth Circuit does not apply the third factor

due to confusion as to its value (*Mollett v. Mullin*, 348 F.3d 902, 920 (10th Cir. 2003)). Other courts have noted the contradiction between the length of the record and the costliness considerations. *See, e.g., United States v. McLaughlin*, 126 F.3d 130, 135 (3d Cir. 1997). As to the second factor, courts have confused the certainty of harmlessness with belief in the defendant's guilt. *See, e.g., United States v. Adams*, 1 F.3d 1566, 1575-76 (11th Cir. 1993). The *Giovannetti* rule's lack of clear standards regularly results in disagreements within three-judge panels. *See, e.g., United States v. Little*, 829 F.3d 1177, 1187-90 (10th Cir. 2016) (Holmes, J., dissenting); *United States v. Montgomery*, 100 F.3d 1404, 1408 (8th Cir. 1996) (Beam, J., dissenting); *United States v. Holly*, 488 F.3d 1298, 1311-13 (10th Cir. 2007) (Kelly, J., dissenting); *United States v. Rodriguez-Preciado*, 399 F.3d 1118, 1133-43 (9th Cir. 2005), *amended*, 416 F.3d 939 (9th Cir. 2005) (Berzon, J., dissenting in part).

2. *The Giovannetti Rule Constitutes An Unauthorized Departure From This Court's Precedent That Places The Burden Of Proving Harmless Error On The Government.*

The *Giovannetti* rule cannot be reconciled with this Court's holdings in *Chapman* and *Kotteakos* that place the burden of proving harmlessness on the government. As found by a court that rejects the *Giovannetti* rule, when the government fails to raise harmlessness, it neither assumes nor carries any burden of proof. *State v. Hill*, 161 Idaho 444, 387 P.3d 112, 118 (2016) ("The State fails to meet its burden of proving harmless error if it does not address the subject in its briefing.").

In *Hill*, the Supreme Court of Idaho reasoned directly from *Chapman* that a preserved constitutional error requires reversal unless the prosecution proves "beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained." *Hill*, 387 P.3d at 118

(quoting *Chapman*, 386 U.S. at 24). In *Hill*, the court made clear that the government’s failure to raise harmlessness categorically defeats any claim that it proved harmlessness beyond a reasonable doubt. 387 P.3d at 117-18. The Supreme Court of Idaho had previously considered and rejected the *Giovannetti* rule in *State v. Almaraz*, 154 Idaho 584, 598-99, 301 P.3d 242, 256-57 (2013). The Idaho court’s rejection of sua sponte harmlessness determinations matches this Court’s application of its precedent in *Hitchcock v. Dugger*, where the State’s failure to argue harmlessness required reversal of the death sentence. 481 U.S. 393, 399 (1987).

Adherence to *Chapman* and *Kotteakos* favors judicial neutrality by requiring the parties to frame the issues. Sua sponte review places judges in a partisan role. When a court addresses harmlessness sua sponte, it is the court of appeals – not the government – that asserts a defense to reversal of the conviction. *See Wood v. Milyard*, 132 S. Ct. 1826, 1833-34 (2012) (courts of appeals abuse their discretion by sua sponte addressing non-jurisdictional defenses that the government knowingly waived). The text of Rule 2 cannot be read to support a drastic departure from the judicial role as neutral arbiter between contesting parties. *See Caperton v. A.T. Massey Coal Co.*, 556 U.S. 868, 876 (2009) (a neutral decision-maker is a “basic requirement of due process”) (quoting *In re Murchison*, 349 U.S. 133, 137 (1955)); *Greenlaw v. United States*, 554 U.S. 237, 243 (2008) (in our adversary system, “we rely on the parties to frame the issues for decision and assign to courts the role of neutral arbiter of matters the parties present.”). This Court’s precedent on harmless error also protects the Sixth Amendment by avoiding the appearance or reality of judicial encroachment upon the jury’s role as the sole determiner of guilt. *See Bumper v. North Carolina*, 391 U.S. 543, 550 n.16 (1968) (“But it is

not the function of this Court to determine innocence or guilt, much less to apply our own subjective notions of justice. Our duty is to uphold the Constitution of the United States.”).

This Court’s exercise of its supervisory authority to reject the *Giovannetti* rule is especially appropriate because the rule takes as its guiding value economic efficiency, with an emphasis on the costs of retrial and deterrence. Richard A. Posner, *Excessive Sanctions for Governmental Misconduct in Criminal Cases*, 57 Wash. L. Rev. 635, 645 (1982) (“What the harmless-error rule does, then, is to identify a type of governmental misconduct whose social costs are much lower than the social costs of attempting to deter the misconduct by overturning the conviction and forcing a retrial.”). This law and economics rationale regards this Court’s precedent on harmless error as “anomalous.” See Richard A. Posner & William M. Landes, *Harmless Error*, 30 J. Legal Stud. 161, 172 (2001) (“But the survival of the [*Chapman*] rule in cases of direct appeal is anomalous in terms of our analysis. For there is nothing in the nature of a constitutional error that makes it affect any of the variables in our model.”). Formulating a rule based on “third party interests” is inimical to the adversarial system that provides the “very premise” of constitutional criminal procedure. *Herring v. New York*, 422 U.S. 853, 862 (1975).

Certiorari should be granted because sua sponte consideration of harmlessness under the *Giovannetti* rule undermines the harmless error standard this Court articulated in *Chapman* and *Kotteakos*.

3. *If Sua Sponte Harmless Error Review Is Ever Permissible In The Direct Review Of Criminal Cases, This Court Should Reject The Giovannetti Rule And Articulate A Clearer Standard.*

The lack of precision in the Seventh Circuit’s formulation of the *Giovannetti* rule has led to ambiguity in its application. For example, does the short length of a trial favor sua sponte review because the record is simple, or does a long trial favor sua sponte review because the affirmance might avoid a protracted and costly retrial? How does a court determine whether harmlessness is “certain or debatable” when the parties have not briefed the issue?

If the Court determines that sua sponte harmless error review is permissible, the Court should exercise its supervisory power to articulate a more workable and narrow standard. As presently exercised, the *Giovannetti* rule is vague and subjective. *See Hanna v. Plumer*, 380 U.S. 460, 463 (1965) (granting certiorari “[b]ecause of the threat to the goal of uniformity of federal procedure posed by the decision below[.]”); *Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 523 U.S. 26, 35 (1998) (the Court addressed and abrogated litigation procedure despite “longstanding practice under the statute and the rule”). The *Giovannetti* factors inject irrelevant considerations into the equation, such as the judges’ opinion as to guilt (futility) and the length of proceedings (costliness). This Court should articulate a rule based on uniform and clear criteria to mitigate its effect on judicial neutrality.

First, any sua sponte judicial review should assume all facts and inferences in the light most favorable to the defense. *See Delaware v. Van Arsdall*, 475 U.S. 673, 684 (1986) (in assessing whether erroneous limitation of cross-examination is harmless, court must “assum[e] that the damaging potential of the cross-examination were fully realized”). The Court should also emphasize that the only relevant factor is whether the error might have affected the jury.

Chapman, 386 U.S. at 23-24 (“An error in admitting plainly relevant evidence which possibly influenced the jury adversely to a litigant cannot . . . be conceived of as harmless.”); *Weiler v. United States*, 323 U.S. 606, 611 (1945) (courts are not authorized to “reach the conclusion that the error was harmless because we think the defendant was guilty”); see *Satterwhite v. Texas*, 486 U.S. 249, 258-59 (1988) (the question is “whether the State has proved beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained”).

Second, the costliness of further proceedings should be removed from the calculus. No defendant, nor any parent of a defendant, should be told that we can afford to imprison a young man for decades, but we cannot afford to assure a fair trial. Cost is an especially inappropriate consideration because it cannot be predicted. The reversal of a jury verdict often results in a resolution short of retrial – dismissal of the charges, a plea agreement with both parties better informed of the risks, or a less costly bench trial sometimes based on stipulated facts. Nor should the length of the trial make a difference in the determination whether to engage in sua sponte harmless error review because of its inherent ambiguity and subjectivity.

This Court formulated single and uniform rules for constitutional and non-constitutional trial errors in *Chapman* and *Kotteakos*. This Court should grant certiorari to vindicate its precedent and to assure that appellate rules of general application are properly promulgated and fair.

4. *The Present Case Provides An Ideal Vehicle For Review Of An Exceptionally Important Issue That, By Its Nature, Avoids Adversarial Appellate Review.*

The present case perfectly illustrates the inconsistency between this Court’s precedent and the *Giovannetti* rule. The prosecution appeared to make a conscious decision to argue

harmlessness on one issue and not on others, and the court's decision to nonetheless affirm a tainted conviction based on harmlessness required it to take on a partisan role. In applying the *Giovannetti* rule to Mr. Mohamud's defense, the Ninth Circuit did not provide any factual analysis whatsoever. The Ninth Circuit's recognition that the defense presented a "solid case for entrapment," combined with its assertions that the harmlessness of multiple errors regarding key disputed issues was "not reasonably debatable" and "further litigation would be futile," indicates that the Ninth Circuit may have resolved disputed facts and inferences in favor of the government, conflating sufficiency review with harmlessness review. *See United States v. Ford*, 550 F.3d 975, 1001 n.9 (10th Cir. 2008) (Gorsuch, J., dissenting) (in reviewing materiality in an entrapment case, "the court again seems to conflate a sufficiency claim with a *Brady* claim").

The Ninth Circuit's apparent conflation of sufficiency and harmlessness analyses is reflected in its sufficiency analysis of entrapment as a matter of law. The Ninth Circuit found that Mr. Mohamud demonstrated no reluctance to become involved in domestic terrorism. App. 22, 27. But reluctance was contested at trial. The defense argued that Mr. Mohamud showed no interest in the six months of provocative emails from government agent Bill Smith expressing his desire to "bring the West to its knees." Then, once the Bill Smith emails had proved fruitless, Mr. Mohamud initially declined to meet with Youssef, saying basically "don't call me, I'll call you." The agents in the next email suggested that God had a purpose for Mr. Mohamud in the United States. Even that email required a reminder before Mr. Mohamud responded. While the Ninth Circuit's sufficiency ruling found no reluctance in the light most favorable to the government, the jury could have reached a different conclusion.

Without conflation of sufficiency and harmlessness, examples abound to demonstrate why the district court's "state of mind" rulings prejudiced Mr. Mohamud's entrapment defense. For example, the Ninth Circuit agreed that the "color commentary" offered by the government agents interpreting what Mr. Mohamud "meant" or was "thinking" during recorded statements was irrelevant speculation. Yet the government was allowed through that testimony to inform the jury that Mr. Mohamud "wanted to commit a terrorist act," that he wanted to "place a device at Pioneer Square," and that his reference to "jihad" in a pre-contact communication meant his plan to join a "terrorist organization" in Somalia, even though Mr. Mohamud himself did not say these things. The admission of the undercover agents' inflammatory opinions objectively had the potential to adversely influence the jury under the proper view of the *Chapman* standard.

The erroneous admission of the Interpol Red Notice was especially prejudicial on the crucial point of predisposition. In pretrial litigation in which the defense sought to exclude all reference to the Notice, the prosecution argued that Al-Ali's role constituted "a key piece of the government's case" and characterized the document as "integral" to the government's case on predisposition. District Court Dockets 374 at 48, 438 at 62. The prosecutor used the Notice for its truth in his opening statement – prior to any defense argument that could have opened the door – by highlighting Mr. Mohamud's connection to Al-Ali, then characterizing Al-Ali as "wanted by the Saudi government" and an "al-Qaeda recruiter." Reliance on the Notice for its truth allowed agents to repeatedly refer to Al-Ali as a terrorist recruiter, and "thus spread before [the jury] damning information that is not subject to cross-examination," which went "far toward abrogating the defendant's rights under the sixth amendment." *Ocampo v. Vail*,

649 F.3d 1098, 1110 (9th Cir. 2011) (quoting *United States v. Silva*, 380 F.3d 1018, 1020 (7th Cir. 2004)). The Notice itself – with its prejudicial testimonial hearsay – accompanied the jurors into their deliberations.

The state of mind errors were pervasive and went to the heart of the entrapment defense because they had the potential to influence the jury on the key point of predisposition. *Compare* District Court Docket 455 at 283 (defense opening statement) *and* District Court Docket 467 at 2598-663 (defense closing argument) *with* Opening Brief, Ninth Circuit Docket 88-1, at 104-28 (description of pervasive trial errors). The Ninth Circuit recognized that the aggressive government conduct and the defendant’s lack of means or intent to commit the crime before the first government contact created a solid case for entrapment. Yet the Ninth Circuit did not even attempt to provide an explanation for its extraordinary conclusion that harmlessness was “not reasonably debatable.”

The government had a heavy burden of negating entrapment beyond a reasonable doubt. The jury note asking about the precise standard for predisposition indicated at least some concerns with the evidence presented. Given the entire context of the trial and the repeated evidentiary errors, there can be no certainty that the identified errors were harmless. This case provides a perfect vehicle for this Court to bring courts of appeals into conformance with its precedent and require that the prosecution be held to its burden of proving harmlessness. *See, e.g., Arizona v. Fulminante*, 499 U.S. 279, 297-301 (1991) (state failed to establish harmless error where one of two confessions suppressed); *Fahy v. Connecticut*, 375 U.S. 85, 88-90 (1963) (failure to suppress corroborative evidence not harmless).

The appearance of fairness is especially crucial given the national profile of the case, with media coverage often focusing on the government's overreach. *See, e.g.,* Nicolás Medina Mora and Mike Hayes, *The Big (Imaginary) Black Friday Bombing*, BuzzFeed News (Nov. 15, 2015).⁵ The acknowledged evidentiary errors compounded the already existing power imbalance from the trial's secrecy, in which the defense was forbidden access to classified discovery, and the government's primary witnesses were allowed to testify anonymously, insulating them from effective cross-examination. *See Smith v. Illinois*, 390 U.S. 129, 131 (1968) ("To forbid this most rudimentary inquiry [name and address] at the threshold is effectively to emasculate the right to cross-examine itself."). The Ninth Circuit's sua sponte decision to ignore trial error on harmlessness grounds in this context exacerbated the appearance of unfairness created by reliance on secret proceedings.

To preserve the appearance of judicial neutrality and to assure consistent application of procedural rules, only this Court should decide if sua sponte harmless error review of preserved errors by the courts of appeals conforms to its precedent and, if so, what form such review should take.

6. Conclusion

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Dated this 14th day of June, 2017.



Stephen R. Sady
Attorney for Petitioner

⁵ Available at https://www.buzzfeed.com/nicolasmedinamora/did-the-fbi-transform-this-teenager-into-a-terrorist?utm_term=.baXVEeomQ#.sexLR6mOz

FOR PUBLICATION

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

MOHAMED OSMAN MOHAMUD,
Defendant-Appellant.

No. 14-30217

D.C. No.
3:10-cr-00475-KI-1

OPINION

Appeal from the United States District Court
for the District of Oregon
Garr M. King, District Judge, Presiding

Argued and Submitted July 6, 2016
Portland, Oregon

Filed December 5, 2016

Before: Harry Pregerson, Carlos T. Bea,
and John B. Owens, Circuit Judges.

Opinion by Judge Owens

SUMMARY*

Criminal Law

The panel affirmed Mohamed Osman Mohamud's conviction for attempting to detonate a large bomb during the annual Christmas Tree Lighting Ceremony in downtown Portland, Oregon, in violation of 18 U.S.C. § 2332a(a)(2)(A).

The panel held that the district court properly rejected Mohamud's defense of entrapment as a matter of law. The panel could not say that no reasonable jury could have concluded that Mohamud was predisposed to commit the charged offense. Rejecting Mohamud's alternative argument that the case should be dismissed because the government overreached in its "sting," the panel wrote that while the government's conduct was quite aggressive at times, it fell short of a due process violation.

The panel held that, under the circumstances of this case, the district court did not err in denying Mohamud's motion to suppress, based on tardy disclosure, information collected pursuant to § 702 of the Foreign Intelligence Surveillance Act of 1978. The panel wrote that Mohamud cannot demonstrate prejudice, and that the district court did not err in finding that the late disclosure was not due to prosecutorial misconduct.

The panel held that the § 702 acquisition of Mohamud's email communications did not violate the Fourth Amendment. The panel noted that all this case involved was

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

the targeting of an overseas foreign national under § 702, through which Mohamud's email communications were incidentally collected. The panel held that no warrant was required to intercept the overseas foreign national's communications or to intercept a U.S. person's communications incidentally. Assuming that Mohamud had a Fourth Amendment right in the incidentally collected communications, the panel held that the search was reasonable under the Fourth Amendment. The panel wrote that declassified facts foreclosed the argument that the discovery in this case strayed from protecting the country from a terrorist threat into the conduct of foreign affairs. Because no retention and querying of the incidentally-collected communications is at issue in this case, an argument regarding reasonableness was outside the scope of this court's review. The panel held that under the third-party doctrine, Mohamud had a reduced expectation of privacy in his communications to third parties. The panel held that Foreign Intelligence Surveillance Court-approved targeting and minimization procedures, which were followed in practice, sufficiently protected Mohamud's privacy interest, in light of the government's compelling interest in national security.

COUNSEL

Stephen R. Sady (argued), Chief Deputy Federal Public Defender; Mark Ahlemeyer, Assistant Federal Public Defender; Lisa C. Hay, Federal Public Defender; Office of the Federal Public Defender, Portland, Oregon; Steven Toby Wax, Portland, Oregon; for Defendant-Appellant.

Kelly A. Zusman (argued), Appellate Chief; Ethan D. Knight, Pamala R. Holsinger, and Ryan W. Bounds, Assistant United States Attorneys; Billy J. Williams, Acting Assistant United States Attorney; United States Attorney's Office, Portland, Oregon; Joseph F. Palmer, Attorney, Appellate Unit; John P. Carlin, Assistant Attorney General; National Security Division, United States Department of Justice, Washington, D.C.; for Plaintiff-Appellee.

Patrick C. Toomey (argued) and Alex Abdo, New York, New York; Andrew Crocker and Mark Rumold, San Francisco, California; Mathew W. dos Santos, Portland, Oregon; as and for Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Oregon, and Electronic Frontier Foundation.

Joshua L. Dratel, Law Offices of Joshua L. Dratel P.C., New York, New York; John D. Cline, Law Office of John D. Cline, San Francisco, California; for Amicus Curiae National Association of Criminal Defense Lawyers.

OPINION

OWENS, Circuit Judge:

Mohamed Osman Mohamud appeals from his conviction for attempting to detonate a large bomb during the annual Christmas Tree Lighting Ceremony in Pioneer Courthouse Square in downtown Portland, Oregon, in violation of 18 U.S.C. § 2332a(a)(2)(A). We have jurisdiction under 28 U.S.C. § 1291, and we affirm.¹

I. FACTUAL BACKGROUND

A. Mohamud's Activities Before Contact with the FBI

In many respects, Mohamud was like any other American teenager. He liked music, the Los Angeles Lakers, and hanging out with his friends. Born in Somalia, he immigrated to the United States at the age of three, and grew up in the Portland area.

But after a December 2008 incident at London's Heathrow Airport, things changed. Believing that airport security racially profiled him, Mohamud wrote an email in London stating that it is "the evil zionist-crusader lobbyists who control the world," and calling on Allah to send fighters against them. He also created a new email account while in London—truthbespoken@googlemail.com. That email account would play a significant role in the prosecution's case.

¹ We resolve several of Mohamud's arguments in a concurrently filed memorandum disposition.

In 2009, Mohamud began communicating over the Internet with Samir Khan, a United States citizen then living in North Carolina.² Khan published *Jihad Recollections*, an online magazine aimed at English-speaking al-Qaeda supporters. From February to August 2009, Mohamud and Khan exchanged roughly 150 emails, with Mohamud using his truthbespoken email account. Topics included Islamic law and advice about personal relationships. They also outlined Mohamud's support for Osama bin Laden.

During this time period, Mohamud wrote four articles for *Jihad Recollections*.³ Among other things, the articles recommended physical exercise to prepare for war with the West and analyzed Europe's vulnerability to a jihadi attack. Mohamud's initial drafts of these articles contained more incendiary content. For example, Mohamud praised the proficiency of the September 11, 2001, hijackers who "hit them so fast the Americans became dumbfounded," the 2008 Mumbai attackers, who were "a great display of quickly entering the arena of battle and just decimating the kuffar [unbelievers]," and the fighters in Afghanistan who attacked landing American helicopters and then "finish[ed] off the wounded American soldiers." Mohamud also prayed for Allah to help the reader "prepar[e] you to meet Allah as a martyr" and included a photograph of the Twin Towers burning during the September 11th attacks. Khan removed

² The September 2011 drone strike in Yemen that killed Anwar al-Awlaki, an al-Qaeda leader, also killed Khan.

³ Three of the articles were published under the pen name Ibn al-Mubarak. Mohamud was not credited with publishing the fourth article, which appeared in *Jihad Recollections* under a different pseudonym, Abu Talha.

this more inflammatory material from the final versions of Mohamud's articles. On August 15, 2009, Mohamud informed Khan that he would no longer write for *Jihad Recollections* because he was "going through alot [sic] of things and i have a lot of things to do."⁴

Mohamud also struck up a relationship with Amro Al-Ali, a Saudi citizen who Mohamud met at a Portland mosque and who subsequently left the United States.⁵ On August 31, 2009, Al-Ali sent information to Mohamud at his truthbespoken email account about an Islamic school in Yemen. That same day, Mohamud called his father to say that he was leaving the country. His father begged him to stay in the United States, but Mohamud told him it was too late—he had his passport, visa, and ticket ready to go. When his parents confirmed that his passport was missing, they feared that Mohamud might return to Somalia, his place of

⁴ Mohamud also engaged in other pro-jihadi Internet activities. In June 2009, for example, he posted on a website that he was working on an "Islam's [M]ost Wanted List," which would be a "Black list" of people who had "offended Allah."

⁵ Saudi officials suspected Al-Ali had links to terrorist groups, and requested an Interpol Red Notice for his arrest. A Red Notice serves as an international wanted notice and provides information on the identification of fugitives charged with or convicted of serious crimes. Although Interpol will not publish requested Red Notices that violate Interpol's Constitution, which prohibits the organization from undertaking any activities of a political, military, religious or racial character, *see* Interpol Const., art. 3, Interpol does not independently vet the governmental request for a Red Notice for its factual and legal justification. The Red Notice led the FBI to consider Al-Ali a "dangerous [person] overseas" and to view Mohamud's communications with Al-Ali with concern. There was no evidence at trial that Mohamud knew of the Red Notice, which was non-public, or the FBI's interest in Al-Ali.

birth. And when they could not reach Mohamud, they called the FBI and asked an agent to stop their son from leaving the country. Eventually, Mohamud's mother got in touch with her son, scolded him, and brought him home. Mohamud did not actually have a visa or plane ticket, and he returned his passport to his parents. A few days later, Mohamud's father called the FBI agent back and told him that Mohamud had agreed to finish college and would not leave the country until he graduated. He also explained that his son had wanted to go to Yemen to study Arabic and Islam. Mohamud's father forwarded the FBI an email from his son about a school in Yemen, which allowed the FBI to identify Mohamud as the user of the truthbespoken email account.

B. Mohamud Attends College and the FBI Initiates Its Investigation

In September 2009, Mohamud began studying engineering at Oregon State University in Corvallis, where he had a "typical" college experience: he had a roommate, made friends, and attended parties (where he drank alcohol and used marijuana). His activities and religious principles often clashed, and in November 2009 he sought advice from a Muslim website on the difficulties of living a pious life on a college campus.

After the urgent August 31, 2009 call from Mohamud's father, the FBI opened an investigation into Mohamud. Agents conducted physical and electronic surveillance of Mohamud, but did not identify any overtly dangerous communications. The case agent believed that Mohamud's communications lacked "the same radical speak that he had espoused early on when he was communicating with Samir Khan." The agent opined that Mohamud had "left behind his

radical thinking” and was a “pretty manipula[ble], conflicted kid.”

C. The FBI’s First Direct Contacts with Mohamud

In November 2009, a contractor working undercover for the FBI—using the alias “Bill Smith”—emailed Mohamud at his truthbespoken account. Pretending to be an isolated Muslim in eastern Idaho, the contractor asked Mohamud for advice on how to get more involved in “the fight” for the Islamic community, and he stated that he wanted “to help rid the occupiers from [P]alestine.” Although Mohamud gave some general advice to move to a community with more Muslims, take care when talking about such issues online, and look out for “spies,” he never openly encouraged the contractor to commit acts of violence. By May 2010, their email communications had ended.

Mohamud planned to work in Alaska with his college roommate during the summer of 2010. But when his parents brought him to the Portland airport, he was not permitted to fly to Alaska. Instead, FBI agents met with Mohamud and his parents at the airport and questioned them. When asked, Mohamud denied having a ticket or visa to travel to Yemen, or having any interest in jihadi websites. When asked if he knew anyone in Yemen, he said “Amr,” but provided little detail. Mohamud made no mention of his *Jihad Recollections* articles or similar writings. When Mohamud returned home, he drafted a “To do list” which included “Find a job,” “Work till September,” get help from his parents for food and rent, and “you might have to take less classes” at Oregon State.

D. Introduction to FBI Undercover Agent “Youssef”

1. The Initial Email Contacts

On June 23, 2010, an FBI undercover agent, using the alias “Youssef,” emailed Mohamud at his truthbespoken account and instructed him to set up a new “hushmail” email account that would be secure and encrypted. Mohamud responded later that same day: “assalamu alaykum [God be with you] brother how are you[?]” Two days later, Youssef emailed Mohamud again:

Wa alaikoom salem. hamdullah i am good brother thank you for asking. i’m sorry for the delay in our communication, we’ve been on the move. jazakallah khairan for responding so soon. are you still able to help the brothers? in sha’allah, i’ll hear from you soon. Salem, Youssef.

Mohamud responded the same day that he was unable to travel:

i have been betrayed by my family, i was supposed to travel last year but Allah had decreed that i stay here longer than my heart desired. i am trying to find a way to go. i do not think i will be able to go for a while. i need to save up and also clear up somethings [sic]. look for my emails inshallah, i will contact you when i am able to travel. pray for me that allah will free my passage from the lands of the polytheists, peace be upon the

messenger of Allah, his family and his companions.

Three days later, on June 28, 2010, Youssef replied that “Allah (SWT) i’m sure has good reason for you to stay where you are” and asked to meet Mohamud. About two weeks later, when Mohamud had still not responded, Youssef sent a follow-up email. A week later, on July 16, 2010, Mohamud responded and agreed to meet.

Youssef declined Mohamud’s suggestion to meet at the local mosque because he wanted to meet privately and “the kuffar [unbelievers] have eyes and ears in almost all masjids in the US.” Mohamud responded that he would “have a set of questions for you when we meet” to “make [s]ure you are not a spy yourself.” Mohamud also wrote that “amr” (as in Amro Al-Ali) was the only person who could have given Youssef his email address, so he would want to know how Youssef knew Al-Ali as a “precaution.” Youssef praised Mohamud for thinking about security.

2. The First Meeting with Youssef

On July 30, 2010, Youssef met Mohamud for the first time in downtown Portland.⁶ Youssef told Mohamud he was from an “ihataa” (a religious “council”) and was interviewing seven people in the United States and Canada for possible

⁶ Although Youssef was wearing a transmitter and a recording device, the meeting was not recorded because the battery accidentally had been drained. An FBI agent listened to their conversation and summarized it in a report. The agent could not hear the first ten minutes, so he relied on Youssef to tell him what occurred. Every other in-person meeting between Mohamud and undercover agents was recorded and proffered as evidence at trial.

inclusion in a council project.⁷ Youssef asked Mohamud “what he had been doing lately to continue being a good Muslim.” Mohamud said that he had been writing poetry and articles for *Jihad Recollections*. Mohamud asked Youssef how he got his email address, and Youssef explained that the council had forwarded it to him.

When asked about travel, Mohamud described his unsuccessful attempt to go to Alaska. And when asked what he was “willing to do for the cause,” Youssef testified that Mohamud said that “originally he had planned to wage war within the United States,” but then he dreamt that he traveled to Yemen, received training, and “went to Afghanistan where he led an army against the kuffar or the unbelievers.”

Youssef asked Mohamud again what he would do for the cause, and Mohamud responded, “anything.” When offered five ways to be a good Muslim—(1) pray five times a day; (2) go to school to learn something that would help the brothers overseas, such as engineering or medicine; (3) raise money for the brothers; (4) become operational; or (5) become a martyr—Mohamud almost immediately picked “become operational.” Mohamud explained “operational” meant “doing like the other brothers do when they get a car, fill it with explosives, park it near a target location, and detonate the vehicle.” When asked about targets, Mohamud said he had thought about Washington, D.C., because of all the government buildings, but admitted he was not familiar with the area. Youssef told Mohamud to research possible

⁷ The FBI invented this “council” to serve as a fictional intermediary between Al-Ali and Youssef because Youssef would not be able to answer many questions about Al-Ali.

targets in Portland, and that he had a “brother that could help him with explosives.”

About four hours after their meeting, Mohamud sent Youssef an unprompted email with copies of his three articles published in *Jihad Recollections*.⁸ Youssef replied that Mohamud was “talented.”⁹

E. Meeting with “Hussein”

A few weeks later, on August 19, 2010, Youssef met with Mohamud again in downtown Portland and introduced him to “Hussein,” an undercover FBI agent posing as an al-Qaeda explosives expert. Youssef described Mohamud as a “jewel in the rough.” During the meeting, Mohamud told the agents he admired the Mumbai terrorist attack (in which ten men stormed buildings in Mumbai, India, and killed 164 people).

About thirty-four minutes into the meeting, Mohamud told the agents that he wanted to detonate a bomb in Pioneer Courthouse Square during the annual Christmas Tree Lighting Ceremony on November 26, 2010, the day after Thanksgiving. Mohamud explained that he had researched other potential targets, but this was the best option because:

⁸ Mohamud also sent Youssef an article he had recently submitted to *Inspire*, the successor to *Jihad Recollections*, observing that: “Much can be done to hurt the enemy or prepare for Jihad. According to your circumstances you could perform Jihad against the enemy where you are currently living by Mumbai style attacks, but my article is directed towards those brothers waiting to travel to the lands of Jihad rather than touch upon the issue of attacks within the Western nations.”

⁹ The undercover agents frequently flattered and praised Mohamud for his good writing or behavior.

(1) he could drive a car right into the Square from the street; (2) many people would be there; (3) nobody expected an attack in Portland; and (4) security would be light. Mohamud said that he planned on being in the car when it blew up. The agents (who were not familiar with Portland) had no input into Mohamud's chosen target.

Youssef wanted Mohamud to realize the seriousness of what he was saying. Mohamud assured them he did. He said that "since I was fifteen I thought about all this things before," and explained:

[I]magine every day we see you know in Arab, you know, newspapers and news you know our people are killed you know. So for us to see that you know it would be a smile from me to see them in the same. You know, you know what I like, what makes me happy? You know, what I like to see? Is when I see the enemy of Allah then they are you know their bodies are torn everywhere. . . . That gives me you know like high hope and happiness you know.

When Youssef pointed out that there would many women and children at the event, Mohamud responded:

[I]n general just a huge mass that will, you know like for them you know to be attacked in their own element with their families celebrating their holidays. And then for later on to be saying this was done for you to refrain from killing our children, women.

The agents told Mohamud there was “no shame” in not going through with his plan. They reminded him that “[w]ith us you always have a choice.” When asked what he would have done if he had not met the agents, Mohamud said that he had planned to leave the country, “find the right people,” “be somewhere they cannot capture you,” and meet up with Al-Ali. The three then walked to Pioneer Courthouse Square, where Mohamud detailed the proposed attack.

Two days later, Youssef emailed Mohamud that he and Hussein would present Mohamud’s plan to the “council.” He also asked Mohamud to explain his rationale for the attack, as “a bomb is a very serious matter.” Mohamud replied that he had prayed for guidance and that his faith “was sky high for no apparent reason,” which he saw as a sign “that the traffic[] [l]ight is green lol.”

F. Youssef and Hussein Test Mohamud’s Resolve

On September 7, 2010, Youssef and Hussein met again with Mohamud. They convinced Mohamud not to martyr himself (i.e., to detonate the bomb remotely), and offered to help him leave the country after the bombing. They also advised that he did not have to go forward with the plan. The agents showed Mohamud an FBI-produced mock jihadi training video, which included an explosion being triggered by cell phone. Mohamud said the video was “beautiful.”

To test his resolve, the agents gave Mohamud \$2,800 to carry out specific tasks: purchase a list of bomb components, decide where to park the van with the bomb, and rent his own

apartment.¹⁰ On October 3, 2010, they again met with Mohamud and told him to rent a storage unit for the van. Mohamud completed these tasks.

G. The Test Bomb

On November 4, 2010, Mohamud, Youssef, and Hussein drove to the Oregon countryside to explode a test bomb. On the drive, when asked what he wanted to do once he was overseas, Mohamud first said he wanted to learn Arabic, and later that he wanted to learn “the inside and out of weaponry” and “bomb-making.” When asked whether he saw himself teaching, he said he also wanted to teach “special operations,” and specialize in “making the enemies you know afraid.” During this conversation, Mohamud stated that “these people who live in this country are the most evil people on earth.”

Hussein again advised that Mohamud did not have to go through with the bombing. Mohamud ignored him, instead commenting on the irony of the term “Black Friday,” the day after Thanksgiving. When asked if he had told anybody about the plan, Mohamud responded that his image was “just a college student” and “nobody even knows that I have you know, that I’m inclined toward jihad, or even towards even like being Islamic.”

To test the bomb, Mohamud pushed buttons on a cell phone, which appeared to trigger an explosion, though an FBI agent actually detonated the bomb. After the explosion, Mohamud said “God is great” in Arabic, that he felt “good,”

¹⁰ Youssef explained that the FBI did not want Mohamud to have a roommate because it would be easier to maintain surveillance and reduce the chance that Mohamud would take matters into his own hands.

and that the bomb test was “just motivation for me.” When Youssef and Hussein asked if he had ever seen dead bodies, Mohamud responded that he thought it was “awesome” when people were jumping from skyscrapers during the September 11th attacks.

On the ride home, Youssef suggested that Mohamud make a “good-bye” video to explain his actions because it could be “inspirational.”¹¹ Mohamud ultimately agreed and wrote a script for the video using topics Youssef suggested.

Mohamud made the video later that day, and explained that this is a “message . . . to those who have wronged themselves.” He described the “dark day” that was coming, and said that no one would be safe “for as long as you threaten our security.” He said that living in the United States “is a sin,” and urged that Muslim parents living in the West not do what his did to him—that is, not “hold others back from completing their obligation” to Allah. Mohamud finished by reading his own poem that extolled the virtues of Muslims and jihad, and ended with a call to:

Carry on oh brothers, and march on ahead to
meet your creator and lie on silk beds, and the
martyrs don’t die, so don’t say they’re
dead. . . . Explode on these kuffar
[unbelievers]. Alleviate our pain. Assassinate
their leaders, commanders, and chiefs. From
your brother to his brother a poem in brief.

¹¹ On cross-examination, Youssef agreed that he had his “finger on the scale” and was trying to influence Mohamud to make the video, and that Mohamud initially wanted to wait to make the video until he was abroad.

H. The Final Countdown

About a week after the test bomb, Mohamud exchanged emails with a friend in Afghanistan. On November 13, 2010, the friend asked Mohamud to “investigate” predator and reaper strike drones to figure out “how to down them.” On November 17, 2010, Mohamud responded: “[D]on’t worry, brother, I will find you something inshallah. Please do not e-mail this email any longer. If someone replies from now on from this e-mail is not me, Remember that. I hope we meet again soon inshallah.”

On November 18, 2010, an excited Mohamud met with Youssef and Hussein for six hours. They went to the storage unit Mohamud had rented, which he had selected in part because there were no surveillance cameras. The three then drove to a hotel in Portland, where Mohamud showed the agents potential parking spots he had researched on his computer. Next, they walked to Pioneer Courthouse Square to discuss the plan further.

During the November 18th meeting, Youssef asked: “What’s a victory gonna be for you?” Mohamud replied: “Try to get most, the most casualties.” Mohamud thought the bombing would get a lot of publicity because “America’s boasting it so ‘oh we haven’t been attacked since 9/11.’” Hussein asked Mohamud if he had any doubts about the bombing. He did not.

On November 23, 2010, Mohamud and Hussein went to the storage unit to see the bomb parts. Mohamud helped load purported bomb parts into Hussein’s car, including barrels, wires, and nails. Mohamud also provided Hussein with items for their disguises to pose as water workers.

On November 25, 2010, Thanksgiving Day, Mohamud drove to Portland and spent the day with friends. His friends said he seemed “happy,” although at dinner he became “reserved.” They all went shopping at an outlet mall that night.

I. “Black Friday”—November 26, 2010

Early the next morning, on November 26th, Mohamud ran into a friend and told him that “I’m having the greatest morning of my life.” Around noon, Youssef picked up Mohamud and they drove to a store to buy reflective vests as part of their disguises. Then they met up with Hussein in downtown Portland. Mohamud appeared “happy” and “excited.”

The three drove about a mile to the parked van. When shown the “bomb” in the back of the van (which an FBI agent had constructed to look real but which was, in fact, inert), Mohamud said it was “beautiful.” They returned to their hotel, ate, talked, and prayed. Shortly before 5:00 p.m., the three drove to the van. Youssef dropped off Mohamud and Hussein, then drove to a pre-arranged meeting location a few blocks west of Pioneer Courthouse Square.

Hussein and Mohamud drove the van to Pioneer Courthouse Square. Before exiting the van, Hussein told Mohamud to connect the wires for the detonator to work. Mohamud did so, and then they walked several blocks to join Youssef in his car. The three drove toward a train station, dropped off Youssef, and then Hussein and Mohamud parked a few blocks from the station.

Mohamud pulled out the cell phone and Hussein read him the number to dial to detonate the bomb. When Mohamud dialed the number and nothing happened, Hussein suggested that they step out of the car for better reception—the arrest signal. Mohamud was dialing the number into the cell phone a second time when FBI agents arrested them both. Hussein was shouting “Allahu Akbar! [God is great]” as he was being arrested. Mohamud was quiet initially, but during transport he began to kick and had to be restrained. Later, when speaking with the jail’s psychiatric nurse, Mohamud cried and said he could not understand “how he had gotten from just being a student to being labeled a terrorist in jail.”

Agents found an undated email printout from Al-Ali in Mohamud’s wallet. A search of Mohamud’s computer revealed videos of the 2007 and 2008 Portland Christmas Tree Lighting Ceremonies, as well as an al-Qaeda video, an audio file titled “No Peace with the Jews,” and numerous references to the word “jihad.” In a notebook found in his apartment, Mohamud had written: “Non Muslims are the eternal enemies of Islam and they must be subdued and humiliated.” He also described the need to “mistrust” everyone and to act normal “to secure myself from the FBI.”

II. PROCEDURAL HISTORY

A. Indictment and Trial

A one-count indictment charged Mohamud with attempted use of a weapon of mass destruction in violation of 18 U.S.C. § 2332a(a)(2)(A). After several years of pretrial litigation and review of immense discovery (including considerable litigation under the Classified Information Procedures Act, 18 U.S.C. app. 3), trial began in January

2013 and lasted thirteen days. Both sides called numerous witnesses, and the cross-examinations were sharp and thorough.

There was no dispute that Mohamud had tried to blow up Pioneer Courthouse Square while it was filled with people. The spirited (and supportable) defense was entrapment—Mohamud, a teenager with no criminal record, had neither the means nor the intent to commit domestic terrorism until he became involved with the undercover FBI contractor (Bill Smith) and FBI agents (Youssef and Hussein). The government countered that Mohamud’s actions before any contact with the FBI—including his *Jihad Recollections* articles—as well as his readiness to commit such a horrific act of violence proved that he had the necessary predisposition to commit the crime. After the close of evidence and argument, the jury returned a guilty verdict, rejecting the entrapment defense.

B. Post-Trial Motions

Mohamud challenged his conviction on numerous grounds. He cited *Sherman v. United States*, 356 U.S. 369 (1958), to argue that the government had entrapped him as a matter of law. Mohamud contended that he had intended to complete college in the United States, and only the FBI’s aggressive and coercive actions had led him down the bombing path. The district court rejected that argument, pointing to evidence that before any contact with the FBI, Mohamud: (1) originally planned to wage war in the United States until a dream refocused him on Yemen; (2) wrote articles for *Jihad Recollections* which advised how best to prepare to carry out “jihad” on non-believers; and (3) had lengthy email conversations with men that the FBI believed

promoted terrorism. The court also highlighted that Mohamud never showed any reluctance (unlike the defendant in *Sherman*), and only thirteen minutes after meeting Youssef in person, he said that he wanted to become “operational” by using a car bomb.

After the verdict (but before sentencing), the government filed a supplemental notice that it had “offered into evidence or otherwise used or disclosed in proceedings, including at trial” information derived from information collected pursuant to § 702 of the Foreign Intelligence Surveillance Act of 1978 (“FISA”), 50 U.S.C. § 1881a (hereinafter referred to as “§ 702”).¹² Mohamud argued that this late notice warranted suppression of this evidence (and any fruits thereof). The government countered that FISA did not provide for suppression in these circumstances, and in any case, there was no substantial prejudice, as the district court could conduct a post-trial suppression analysis. The district court agreed, finding no misconduct in the late disclosure, and that Mohamud had suffered no prejudice from the delayed disclosure.

Mohamud also argued that suppression was warranted because § 702 violates the First and Fourth Amendments, as well as the separation of powers doctrine.¹³ As a threshold

¹² Section 702 was added to by the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, and was amended by the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

¹³ Here, Mohamud contended that U.S. Foreign Intelligence Surveillance Court (“FISC”) review of targeting and minimization procedures under § 702 amounts to “providing a non-judicial advisory opinion” and authorizes a rule-making role for judges in violation of the non-delegation doctrine.

matter, the district court first held that § 702 did not “interfere[] with the prerogatives of another branch of government beyond requiring the executive branch to conform to the statute.” It also reasoned that because the FISC either approves or denies the requested acquisition (and electronic communication service providers must follow the directives or challenge them), its opinions are not advisory. The court then explained that Mohamud had not raised an independent First Amendment claim, because motions to suppress based on First Amendment violations are analyzed under the Fourth Amendment.

Finally, the district court held that § 702 does not violate the Fourth Amendment. The court reasoned that § 702 surveillance does not trigger the Fourth Amendment’s warrant requirement because U.S. persons’ data is collected only incidentally, but even if it did, no warrant would be required because the foreign intelligence exception would apply.¹⁴ The court then balanced the government’s interests in the search against the intrusions on Mohamud’s privacy, and held that the § 702 collection here was reasonable under the Fourth Amendment.

C. Sentencing

The Sentencing Guidelines called for a life sentence. The government recommended a sentence of forty years’ imprisonment, whereas Mohamud urged a sentence of ten years’ imprisonment.

¹⁴ The district court further held that subsequent querying of § 702-acquired data, without obtaining an additional search warrant, would also be constitutional, though it was “a very close question.”

During the sentencing hearing, the district court acknowledged that, although the jury had rejected the entrapment defense, Youssef and Hussein “imperfect[ly]” entrapped Mohamud through their frequent praise and religious references, especially considering his youth. But the “horrific” nature of the intended crime, which would have resulted “in a great deal of death and mutilation,” still warranted a sentence of thirty years’ imprisonment.

III. DISCUSSION

A. Standard of Review

We review the district court’s ruling on a motion for acquittal de novo. *See United States v. Sanchez*, 639 F.3d 1201, 1203 (9th Cir. 2011). When a defendant pursues an entrapment defense, we “should not disturb the jury’s finding unless, viewing the evidence in the light most favorable to the government, no reasonable jury could have concluded that the defendant[] [was] predisposed to commit the charged offenses.” *United States v. Davis*, 36 F.3d 1424, 1430 (9th Cir. 1994). We review the denial of a motion to dismiss based on a violation of constitutional rights de novo. *United States v. Brobst*, 558 F.3d 982, 994 (9th Cir. 2009).

We review de novo the denial of a motion to suppress evidence, but underlying factual findings are reviewed for clear error. *United States v. Crawford*, 372 F.3d 1048, 1053 (9th Cir. 2004) (en banc). We review for an abuse of discretion a district court’s decision whether to use its supervisory powers—in this case, the supervisory power to decide whether to suppress evidence as a sanction for the government’s late supplemental FISA notice. *United States v. Stinson*, 647 F.3d 1196, 1209 (9th Cir. 2011). Discovery

rulings and the denial of an evidentiary hearing are also reviewed for an abuse of discretion. *United States v. Mazzealla*, 784 F.3d 532, 537 (9th Cir. 2015).

We review de novo the constitutionality of a statute. *United States v. Vongxay*, 594 F.3d 1111, 1114 (9th Cir. 2010).

B. Entrapment as a Matter of Law

As the district court stated at sentencing, the defense made a solid case for entrapment. But the jury rejected that defense, and found Mohamud guilty despite the actions and encouragement of Youssef and Hussein and the communications (and attempted communications) from other government agents. And in light of that verdict, Mohamud has a steep hill to climb. “To establish entrapment as a matter of law, the defendant must point to undisputed evidence making it patently clear that an otherwise innocent person was induced to commit the illegal act by trickery, persuasion, or fraud of a government agent.” *United States v. Smith*, 802 F.2d 1119, 1124 (9th Cir. 1986); *see also United States v. Williams*, 547 F.3d 1187, 1197 (9th Cir. 2008).

To avoid a finding of entrapment, the government must prove that: (1) Mohamud was predisposed to commit the crime before government agents contacted him, or (2) government agents did not induce him to commit the crime. *United States v. McClelland*, 72 F.3d 717, 722 (9th Cir. 1995). We focus our inquiry on Mohamud’s predisposition.

When evaluating predisposition, we often analyze five factors: (1) the character and reputation of the defendant;

(2) whether the government made the initial suggestion of criminal activity; (3) whether the defendant engaged in the activity for profit; (4) whether the defendant showed any reluctance; and (5) the nature of the government's inducement. *Id.* "Although none of these factors is controlling, the defendant's reluctance to engage in the criminal activity is the most important." *Id.*

We can assume that factors (1), (3), and (5) are in Mohamud's favor. The second factor—whether the government made the initial suggestion of criminal activity—weighs against Mohamud. Although Youssef discussed with Mohamud five options of how to be a good Muslim, including the option to become "operational," Mohamud—not Youssef—made the initial suggestion to fill a car with explosives near a target location. Mohamud also told Youssef that he wanted to "wage war" within the United States before Youssef mentioned the possibility of an "operational" role. The government can rely upon Mohamud's statements to prove predisposition even though he made them after the initial contact by the government. *United States v. Tucker*, 133 F.3d 1208, 1217 (9th Cir. 1998).¹⁵ Here, Mohamud discussed placing explosives in vehicles near target locations after the government's initial

¹⁵ In *Tucker*, a jury convicted the defendant of extortion and filing false tax returns. This court affirmed his conviction and sentence, and rejected his argument that the evidence proved entrapment as a matter of law. This court considered statements made by the defendant even after the initial contact between the defendant and the government, noting that "[t]o prove the defendant's predisposition, the government can rely upon evidence occurring after the initial contact with a government agent." *Tucker*, 133 F.3d at 1217.

contact with him but before Youssef suggested criminal activity. The second factor therefore weighs against Mohamud.

The fourth and “most important” factor also weighs overwhelmingly in the government’s favor. The government initiated its contact with Mohamud in November 2009 with the Bill Smith emails, and the more aggressive Youssef and Hussein operation began in June 2010. Despite being provided numerous opportunities to deviate from or terminate the plan, Mohamud never displayed any reluctance in going through with a horrific attack that would have killed and maimed countless people, including young children. Indeed, he expressed great enthusiasm in seeing it through. He picked the target—the Pioneer Courthouse Square Christmas Tree Lighting Ceremony—and planned where the van containing the explosives would be parked. He praised the terror attack in Mumbai, described the victims jumping from the Twin Towers on September 11th as “awesome,” and stated that he would be “happy” to see the bodies of “enemies of Allah” torn apart.

The complete lack of reluctance on Mohamud’s part to participate in the bombing—indeed, his immediate zeal to see it through—separates this case from those in which courts have found defendants entrapped as a matter of law. For example, in *Jacobson v. United States*, 503 U.S. 540, 553 (1992), Jacobson was not predisposed in part because “[t]he evidence that [Jacobson] was ready and willing to commit the offense came only after the Government had devoted 2 ½ years to convincing him that he had or should have the right to engage in the very behavior proscribed by law.” In *Sherman*, a government informant approached the defendant, a recovering drug addict, and asked for narcotics, ostensibly

because the informant was not responding to treatment. 356 U.S. at 371. The defendant resisted—“[f]rom the first, [he] tried to avoid the issue.” *Id.* Only “after a number of repetitions of the request, predicated on [the informant’s] presumed suffering, did [the defendant] finally acquiesce.” *Id.*; *see also id.* at 373 (“One request was not enough, for . . . additional ones were necessary to overcome, first, [the defendant’s] refusal, then his evasiveness, and then his hesitancy in order to achieve capitulation.”). And in *United States v. Poehlman*, 217 F.3d 692 (9th Cir. 2000), the government agent aggressively pushed the idea of sexual activities with children on an uninterested defendant until eventually he gave in:

While Poehlman’s reluctance might have been borne of caution . . . the fact remains that Poehlman’s earliest messages (which would be most indicative of his pre-existing state of mind) provide no support for the government’s case on predisposition. To the contrary, Poehlman’s reluctance forced [the agent] to become more aggressive in her suggestions

Id. at 704; *see also id.* at 695–97. At least as to this factor, this case is more akin to *Williams*, in which we held that the defendant was not entrapped as a matter of law in part because “[t]here is no evidence that [the defendant] expressed any reluctance about the robbery that needed to be ‘overcome by repeated government inducement or persuasion.’ The evidence indicated that [he] was ready and willing at all times to participate in the robbery.” 547 F.3d at 1198 (citation omitted).

Mohamud argues that his actions after the Bill Smith emails are irrelevant for entrapment purposes, as they were tainted by the government's overwhelming inducement. And with those post-Bill Smith actions set aside, the argument goes, there was insufficient evidence for the jury to conclude that he had the necessary predisposition to commit this crime. This is wrong for two reasons.

First, although “only those statements that indicate a state of mind untainted by the inducement are relevant to show predisposition,” statements made after the inducement which make “clear that [Mohamud] would have committed the offense even without the inducement” are evidence of predisposition. *Poehlman*, 217 F.3d at 704–05. This would include Mohamud's statements that he made about the “awesome” terrorist attacks in Mumbai and on September 11th, and that he had been thinking about these “things” since he was fifteen years old. And a reasonable jury could infer that his decisions to become “operational” and blow something up the first time he met Youssef (and later, to choose Pioneer Courthouse Square at its most crowded time) were evidence that his predisposition existed long before FBI contractor Bill Smith emailed him.

Second, even if there were a rigid wall between pre- and post-inducement, there was sufficient evidence for a reasonable jury to reject the entrapment defense. Mohamud's *Jihad Recollections* articles—both the draft and final versions—provided ample evidence of his predisposition to carry out the charged crime. In those articles, he, among other things, coached people on how to prepare themselves physically to attack and kill their Western enemies, and saluted those in Afghanistan who “finish[ed] off” wounded American soldiers. Although these articles may come across

as a teenager trying to talk tough, they were enough to support the jury's finding, and for us to conclude that Mohamud was not the "otherwise innocent person" that the entrapment-as-a-matter-of-law doctrine requires. *Smith*, 802 F.2d at 1124; *cf. United States v. Cromitie*, 727 F.3d 194, 207–08 (2d Cir. 2013) (holding that the defendant in a similar case was not entrapped as a matter of law, and observing that "potential terrorists who are available to be recruited by Al Qaeda or similar groups" may not have necessarily already formed a specific plan, but "[t]heir predisposition is to have a state of mind that inclines them to inflict harm on the United States, be willing to die like a martyr, be receptive to a recruiter's presentation, . . . and welcome an invitation to participate").

In addition, the jury learned of Mohamud's correspondence with Al-Ali, which began months before the first contact from Bill Smith. The jury also learned of Mohamud's desire to go abroad and study at the Islamic school in Yemen that Al-Ali recommended to him. A government expert testified that this school was founded by a Muslim cleric who supported jihad and that it served as a "stepping stone" to violent jihad, especially for people from the West. As detailed above, the same day that Al-Ali told Mohamud about the school in Yemen, Mohamud apparently made plans to leave the United States. Though Mohamud ultimately remained in the country, the jury could have reasonably interpreted his attempt as evidence of a predisposition to commit the crime charged. Further, Mohamud continued to demonstrate interest in attending the school in his December 2009 emails to Al-Ali, which occurred after the Bill Smith emails.

In sum, viewing the evidence in the light most favorable to the government, we cannot say that “no reasonable jury could have concluded that [Mohamud was] predisposed to commit the charged offense[.]” *Davis*, 36 F.3d at 1430. We therefore conclude that the district court properly rejected his defense of entrapment as a matter of law.

Mohamud’s alternative argument that we should dismiss this case because the government overreached in its “sting” and violated due process also fails. While the government’s conduct in this case was quite aggressive at times, it fell short of a due process violation.

In *United States v. Black*, we made clear that “[d]ismissing an indictment for outrageous government conduct . . . is limited to extreme cases in which the defendant can demonstrate that the government’s conduct violates fundamental fairness and is so grossly shocking and so outrageous as to violate the universal sense of justice.” 733 F.3d 294, 302 (9th Cir. 2013) (citation and internal quotation marks omitted). This is an “extremely high standard.” *Id.*; see also *United States v. Pedrin*, 797 F.3d 792, 797 (9th Cir. 2015) (“[I]n assessing whether the government’s conduct was ‘outrageous,’ the relevant question is what the government knew when it was setting up the sting, not what it learned later.”). For example, we have denied challenges to sting operations involving armed robberies of phony drug stash houses which necessarily put law enforcement and the defendant in grave peril. See *Black*, 733 F.3d at 302; *Williams*, 547 F.3d at 1200–01. Mohamud argues that the six factors for evaluating outrageous

government conduct set out in *Black* favor dismissal of the indictment.¹⁶ We disagree.

In *Cromitie*, a comparable Second Circuit case, the defendant was convicted of planning and attempting to carry out domestic terrorism offenses. 727 F.3d at 199–204. The defendant claimed that the government’s conduct in persuading him to commit the charged offenses violated due process. *Id.* at 217. The Second Circuit held that it did not. Even though the government “invented all of the details of the scheme,” the defendant’s express desire to “do something to America” and “die like a martyr” was sufficient to justify the government’s testing of how far he would go. *Id.* at 219. Like Mohamud, *Cromitie* argued that the government took advantage of his religious affiliation, but the court explained that a government agent “is entitled to probe the attitudes” of an individual who “volunteers that he wants to ‘do something to America’ . . . to learn whether his religious views have impelled him toward the violent brand of radical Islam that poses a dire threat to the United States.” *Id.* at 219–20.

¹⁶ These factors are analyzed collectively in determining whether government conduct is outrageous: “(1) known criminal characteristics of the defendants; (2) individualized suspicion of the defendants; (3) the government’s role in creating the crime of conviction; (4) the government’s encouragement of the defendants to commit the offense conduct; (5) the nature of the government’s participation in the offense conduct; and (6) the nature of the crime being pursued and necessity for the actions taken in light of the nature of the criminal enterprise at issue.” *Black*, 733 F.3d at 303. The first three are relevant to how the government set up the sting, the fourth and fifth analyze the government’s role in the sting, and the last relates to the justification for the operation. *Id.* at 303–04.

Cromitie further claimed that the government had violated due process because a government informant had exploited his relationship with Cromitie to “manipulate Cromitie into agreeing to the planned attacks”; the court cited our precedent indicating that “the ‘illusory cultivation of emotional intimacy’ does not exceed due process limits.” *Id.* at 220 (quoting *United States v. Simpson*, 813 F.2d 1462, 1467 (9th Cir. 1987)). Even considering certain monetary benefits offered by the government informant—including \$250,000 cash, a barbershop valued at \$70,000, a new BMW, and a two-week vacation—the court held that the overall operation did not rise to the level of a due process violation. *Id.* Although Mohamud may have been more vulnerable than Cromitie, the government’s questionable actions in that case far exceeded anything here.

In light of the extremely high standard set out in *Black*, we hold that the government’s conduct here did not violate due process.

C. Late Notice Of § 702-Derived Evidence

FISA requires the government to “notify the aggrieved person and the court” prior to trial when it intends to use at trial evidence “obtained or derived from electronic surveillance” pursuant to FISA. 50 U.S.C. § 1806(c); *see also* 50 U.S.C. § 1881e(a) (stating that information acquired under § 702 is subject to the notice requirement in § 1806(c)). The government provided a supplemental notice regarding evidence derived under § 702 after the trial concluded. Mohamud argues that this late disclosure mandates suppression, or at a minimum, discovery and an evidentiary hearing to explore the tardy disclosure.

In answering this question, we must keep two principles in mind. First, “[s]uppression of evidence . . . has always been our last resort, not our first impulse.” *Hudson v. Michigan*, 547 U.S. 586, 591 (2006); *see also Davis v. United States*, 564 U.S. 229, 237 (2011) (“For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.”); *Sanchez-Llamas v. Oregon*, 548 U.S. 331, 347 (2006) (“[T]he exclusionary rule is not a remedy we apply lightly.”). Second, Congress has the power to authorize suppression for statutory violations, as it has done elsewhere in FISA. *See* 50 U.S.C. §§ 1806(g), 1825(h), 1845(g) (FISA); *see also* 18 U.S.C. § 2518(10)(a) (Title III wiretap). However, Congress has not mandated suppression as a remedy for late disclosure of a FISA notice, and, indeed, it apparently anticipated the possibility of post-trial notification. *See* 50 U.S.C. § 1806(e) (providing that a motion to suppress “unlawfully acquired” or nonconforming information “shall be made before the trial . . . unless . . . the person was not aware of the grounds of the motion”). These two principles strongly suggest that automatic suppression is not a required remedy for delayed FISA disclosure.

And in any case, Mohamud cannot demonstrate how the late disclosure prejudiced him. As the district court explained, it fully evaluated the § 702-derived evidence as if the motion had been brought before trial. This put Mohamud in the same position he would have been in if the government had provided timely notice.

Moreover, the district court found that the late disclosure was not due to “prosecutorial misconduct.” Rather, the government had changed its legal opinion about when evidence could be considered “derived from” § 702 surveillance, performed another review of this case, and

provided the late supplemental notice on its own initiative. Our review of the unclassified and classified record supports that the district court did not clearly err in finding no prosecutorial misconduct.¹⁷

As the district court recognized, it had the power to suppress evidence, or even dismiss the indictment or grant a new trial, under its supervisory and statutory authority. *See Stinson*, 647 F.3d at 1210 (stating that a court may exercise its supervisory powers “to remedy a constitutional or statutory violation; to protect judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; or to deter future illegal conduct” (citation omitted)); *see also* Fed. R. Crim. P. 16(d)(2). However, the district court determined that suppression as a sanction for the late supplemental FISA notice was not warranted here, and we agree.

We conclude that, under the circumstances of this case, the district court did not err in denying Mohamud’s motion to suppress premised on the late supplemental FISA notice.¹⁸

¹⁷ We do not reach whether suppression is necessary as a deterrent in light of the government’s apparent self-correction of its practices. *See United States v. Dreyer*, 804 F.3d 1266, 1280 (9th Cir. 2015) (en banc).

¹⁸ We also conclude that the district court did not abuse its discretion in denying discovery and an evidentiary hearing to explore the government’s late disclosure. Mohamud’s reliance on *United States v. Hernandez-Meza*, 720 F.3d 760, 769 (9th Cir. 2013), is misplaced because the record here does not “suggest[] that the government may have deliberately withheld” the supplemental FISA notice. Therefore, we decline Mohamud’s alternative request to remand for further fact finding.

D. Section 702 Collection of Mohamud's Email Communications

1. Legal Background

In 1978, Congress enacted FISA “to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1143 (2013) (citing 50 U.S.C. § 1801 *et seq.*). To do so, the government must obtain a FISA warrant from the FISC. *Id.* The FISA Court of Review assesses any denials by the FISC of applications for electronic surveillance. *Id.*

Thirty years later, Congress enacted § 702 as part of the FISA Amendments Act of 2008. 50 U.S.C. § 1881a. Section 702 “supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC’s authorization of certain foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad.” *Clapper*, 133 S. Ct. at 1144. “Unlike traditional FISA surveillance, § [702] does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power.” *Id.* “And, unlike traditional FISA, § [702] does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.” *Id.* Instead, § 702 mandates that the government obtain the FISC’s “approval of ‘targeting’ procedures, ‘minimization’ procedures, and a governmental certification regarding proposed surveillance.” *Id.* at 1145 (quoting 50 U.S.C. § 1881a(a), (c)(1), (i)(2), (i)(3)).

2. No Fourth Amendment Violation

Although § 702 potentially raises complex statutory and constitutional issues, this case does not. As explained below, the initial collection of Mohamud’s email communications did not involve so-called “upstreaming” or targeting of Mohamud under § 702, more controversial methods of collecting information.¹⁹ It also did not involve the retention and querying of incidentally collected communications. All this case involved was the targeting of a foreign national under § 702, through which Mohamud’s email communications were incidentally collected. Confined to the particular facts of this case, we hold that the § 702 acquisition of Mohamud’s email communications did not violate the Fourth Amendment.²⁰

At our request post-argument, the government declassified certain facts about Mohamud’s surveillance. Through the monitoring of a foreign national’s email account,

¹⁹ Under “upstream” collection, entire streams of Internet traffic flowing across major U.S. networks are acquired and searched, as opposed to “PRISM” collection, under which particular user accounts are monitored, and communications to or from those accounts are collected, including communications with U.S. persons. See, e.g., *Privacy & Civil Liberties Oversight Board (“PCLOB”), Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), at 7 (hereinafter “PCLOB Report”); see also *id.* at 33–41 (comparing PRISM and upstream collection).

²⁰ In light of our holding, we do not reach the question of whether the good faith exception to the exclusionary rule provides an independent basis to affirm the district court’s denial of Mohamud’s motion to suppress. See generally *Davis*, 564 U.S. at 240–42; *Illinois v. Krull*, 480 U.S. 340, 349–55 (1987); *United States v. Leon*, 468 U.S. 897, 925 (1984).

the United States government learned that Mohamud was in contact with that foreign national, who was located overseas. This contact—a limited number of emails between Mohamud and the foreign national—was used to obtain a FISA warrant to surveil Mohamud and his activities. None of these emails was introduced at trial.²¹ We permitted the parties to file supplemental briefs to address the facts offered in the post-argument disclosure.

a. No Warrant Required to Intercept Overseas Foreign National's Communications or to Intercept U.S. Person's Communications Incidentally

As a threshold matter, “the Fourth Amendment does not apply to searches and seizures by the United States against a non-resident alien in a foreign country.” *United States v.*

²¹ We address only Mohamud's as-applied challenge. See *United States v. Salerno*, 481 U.S. 739, 745 (1987) (“A facial challenge to a legislative Act is, of course, the most difficult challenge to mount successfully, since the challenger must establish that no set of circumstances exists under which the Act would be valid.”). Though he also purports to challenge § 702 facially, citing *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2451 (2015), Mohamud does not explain why techniques not employed in this case would require suppression of the evidence gathered here. 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. See, e.g., *United States v. Posey*, 864 F.2d 1487, 1491 (9th Cir. 1989) (“[W]e think it clear that appellant may not make a facial challenge to the FISA without arguing that the particular surveillance *against him* violated the Fourth Amendment. . . . Even if he is correct that the FISA's language might be applied in ways that violate the Fourth Amendment, he must show that the particular search in his case violated the Fourth Amendment. Appellant cannot invalidate his own conviction on the argument that others' rights are threatened by FISA.” (emphasis in original)).

Zakharov, 468 F.3d 1171, 1179 (9th Cir. 2006) (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75 (1990)); see also *Verdugo-Urquidez*, 494 U.S. at 274–75 (“At the time of the search, [respondent] was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico. Under these circumstances, the Fourth Amendment has no application.”). Thus, the government’s monitoring of the overseas foreign national’s email fell outside the Fourth Amendment.

Mohamud argues that under *Verdugo-Urquidez*, the location of the search matters, and that here, the searches took place in the United States.²² Indeed, the government acknowledges that “collection from service providers under Section 702 takes place within the United States.” Yet, as one court put it, “what matters here is the location of the *target*,” and not where the government literally obtained the electronic data. *United States v. Hasbajrami*, No. 11-CR-623, 2016 WL 1029500, at *9 n.15 (E.D.N.Y. Mar. 8, 2016) (emphasis in original); see also Kris & Wilson, *National Security Investigations & Prosecutions* § 17:3 (2016) (“For non-U.S. person targets, there is no probable-cause requirement; the only thing that matters is [] the government’s reasonable belief about[] the target’s location.”).

Consistent with *Verdugo-Urquidez* and our precedent, we hold that this particular type of non-upstream collection—

²² Mohamud also argues that the targeted foreign national may have had sufficient “voluntary connection[s]” to the United States for the Fourth Amendment to apply. See *Verdugo-Urquidez*, 494 U.S. at 271, 273. We have reviewed the classified record, and are satisfied that is not the case here.

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 FISA Review Court in *In re Directives Pursuant to Section 105B of FISA*, similarly applied this principle, holding that “incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.” 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008); *see also United States v. Donovan*, 429 U.S. 413, 436 n.24 (1977) (holding that a Title III wiretap warrant is not made unconstitutional by “failure to identify every individual who could be expected to be overheard,” but “the complete absence of prior judicial authorization would make an intercept unlawful”); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) (explaining that “in the Title III context, incidental interception of a person's conversations during an otherwise lawful surveillance” does not violate the Fourth Amendment).

Mohamud and Amici²³ urge us not to apply this “incidental overhear” approach. First, Amici contend that surveillance of U.S. persons' communications under § 702 is not “incidental” because the monitoring of communications between foreign targets and U.S. persons was specifically contemplated and to some degree desired. We agree that such communications were anticipated. As the Privacy and Civil Liberties Oversight Board found with respect to PRISM collection, “[t]he collection of communications to and from

²³ Amici are the American Civil Liberties Union, American Civil Liberties Union of Oregon, and the Electronic Frontier Foundation.

a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons. Such ‘incidental’ collection of communications is not accidental, nor is it inadvertent.” PCLOB Report at 82; *see also* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol’y 117, 159–64, 259–62 (2015) (discussing the relative volume and intrusiveness of surveillance authorized under § 702). 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.

Mohamud and Amici also contend that the “sheer amount of ‘incidental’ collection” separates § 702 from prior cases where courts have found such collection permissible. We agree with the district court’s observation that the most troubling aspect of this “incidental” collection is not whether such collection was anticipated, but rather its volume, which is vast, not *de minimis*. *See* PCLOB Report at 114 (“The term ‘incidental’ is appropriate because such collection is not accidental or inadvertent, but rather is an anticipated collateral result of monitoring an overseas target. But the term should not be understood to suggest that such collection is infrequent or that it is an inconsequential part of the Section 702 program.”). This quantity distinguishes § 702 collection from Title III and traditional FISA interceptions. However, the mere fact that more communications are being collected incidentally does not make it unconstitutional to apply the same approach to § 702 collection, though it does

increase the importance of minimization procedures once the communications are collected.²⁴

Additionally, Mohamud and Amici contend that prior cases upholding incidental collection involved prior judicial review or a “narrowly drawn exception to the warrant requirement,” as opposed to the collection here. *See, e.g., United States v. Kahn*, 415 U.S. 143, 156–57 (1974) (upholding interception of communications of a woman that were incidentally collected under a wiretap order targeting her husband); *United States v. Figueroa*, 757 F.2d 466, 473–75 (2d Cir. 1985) (holding that wiretap order was not made unconstitutional by permitting interception of conversations of “others as yet unknown”); *see also United States v. Martin*, 599 F.2d 880, 884–85 (9th Cir. 1979) (holding that the Fourth Amendment does not require wiretap application to show probable cause that non-targeted individual named as a “probable converser” committed a crime), *overruled on other grounds by United States v. De Bright*, 730 F.2d 1255 (9th Cir. 1984) (en banc). However, the searches in those cases targeted United States citizens and took place within the United States, so a warrant was required for the initial search to be constitutionally permissible. But “the guiding principle behind them applies with equal force here: when surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons’ communications with the targeted persons is also lawful.” *Hasbajrami*, 2016 WL 1029500, at *9.

²⁴ To the extent that Amici argue that the incidental overhear doctrine permits the unconstitutional and widespread retention and querying of the incidentally collected information, that issue is not before us.

For these reasons, and because the target of the surveillance was a non-U.S. person located outside of the United States at the time of the surveillance, the government was not required to obtain a search warrant to collect Mohamud's email communications with the overseas foreign national as an incident to its lawful search of the foreign national's email.²⁵

b. Collection of Mohamud's Emails was Reasonable

Assuming that Mohamud had a Fourth Amendment right in the incidentally collected communications, the search at issue was reasonable under the Fourth Amendment.²⁶

"Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution." *Maryland v. King*, 133 S.

²⁵ Because the incidental collection excepts this search from the Fourth Amendment's warrant requirement, we need not address any "foreign intelligence exception."

²⁶ It is unclear whether Mohamud had a right to bar use of these incidentally-collected communications in evidence against him on the basis that the communications were seized in violation of the Fourth Amendment. Commentators suggest that he does, so we will assume that here. See, e.g., Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 Stan. L. Rev. 285, 313–14 (2015) ("Communicating with a person who lacks Fourth Amendment rights should not waive the rights of the person who has those rights. The Fourth Amendment should continue to fully protect the U.S. person who communicates with those lacking Fourth Amendment rights."); PCLOB Report at 94 ("The government has acknowledged that the Fourth Amendment rights of U.S. persons are affected when their communications are acquired under Section 702 incidentally or otherwise[.]").

Ct. 1958, 1970 (2013). In deciding reasonableness, we examine the totality of the circumstances and weigh “‘the promotion of legitimate governmental interests’ against ‘the degree to which [the search] intrudes upon an individual’s privacy.’” *Id.* (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). We agree with the district court that under these circumstances, the search was reasonable under the Fourth Amendment.

i. Government Interest

“[T]he Government’s interest in combating terrorism is an urgent objective of the highest order.” *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010). Neither Mohamud nor Amici challenge this. Instead, they argue that (1) the statutory definition of “foreign intelligence information” in § 702 is overbroad because it is not confined to national security information but also includes “the conduct of [] foreign affairs”²⁷; and (2) even if national security justifies the initial acquisition, it is unreasonable to then retain and later search U.S. persons’ § 702-acquired communications without a warrant.

The declassified facts foreclose both arguments. First, as the district court observed, “the discovery in this case all concerned protecting the country from a terrorist threat and did not stray into the broader category of the conduct of foreign affairs.” Thus, we need not determine whether the collection of foreign affairs communications is reasonable. Similarly, the second argument is also outside the scope of our review, as no such retention and querying is at issue in this case.

²⁷ See 50 U.S.C. §§ 1801(e)(2)(b), 1881(a).

ii. Mohamud's Privacy Interest

The parties agree that Mohamud had some expectation of privacy in his electronic communications, but disagree as to the strength of his interest. The government argues that U.S. persons have a limited expectation of privacy when communicating electronically with non-U.S. persons located outside the United States because of the Fourth Amendment's "third-party" doctrine—that a person's privacy interest is diminished where he or she reveals information to a third party, even in confidence. Mohamud contends that the voluntary disclosure of information to third parties does not reduce the expectation of privacy. The district court determined that under the third-party doctrine, Mohamud had a reduced expectation of privacy in his communications to third parties. We agree.

With respect to a U.S. person's privacy interest, we treat emails as letters. *See, e.g., [Redacted]*, 2011 WL 10945618, at *26 (FISA Ct. Oct. 3, 2011) ("Whether they are transmitted by letter, telephone or e-mail, a person's private communications are akin to personal papers."); *United States v. Warshak*, 631 F.3d 266, 285–86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."). Accordingly, until electronic communications reach the recipient, they retain the same level of privacy interest as if they were still in the home. *See, e.g., United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970).

But as with letters, "[a] person's reasonable expectation of privacy may be diminished in 'transmissions over the Internet or e-mail that have already arrived at the recipient.'"

United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (quoting *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (citing *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001))); *see also Guest*, 255 F.3d at 333 (“[Users] would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose ‘expectation of privacy ordinarily terminates upon delivery’ of the letter.” (citation omitted)).

It is true that prior case law contemplates a diminished expectation of privacy due to the risk that the recipient will reveal the communication, not that the government will be monitoring the communication unbeknownst to the third party. *See, e.g., United States v. Miller*, 425 U.S. 435, 443 (1976); *United States v. White*, 401 U.S. 745, 752 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966). While these cases do not address the question of government interception, the communications at issue here had been sent to a third party, which reduces Mohamud’s privacy interest at least somewhat, if perhaps not as much as if the foreign national had turned them over to the government voluntarily. *See also Hasbajrami*, 2016 WL 1029500 at *11 & n.18 (observing same distinction).

Thus, Mohamud’s interest in the privacy of his communications received by the overseas foreign national is diminished.

iii. Privacy Protecting Measures

An important component of the reasonableness inquiry is whether the FISC-approved targeting and minimization measures sufficiently protect the privacy interests of U.S.

persons. Targeting and minimization procedures govern, respectively, who may be targeted for surveillance and how intercepted communications are to be retained and disseminated.

In brief, 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.” 50 U.S.C. § 1881a(d)(1). Among other requirements, minimization procedures must be “reasonably designed” “to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” 50 U.S.C. §§ 1801(h)(1), 1881a(e)(1).

After evaluating the protections detailed in § 702 and the classified minimization procedures, the district court concluded that as applied to Mohamud, § 702 is reasonable under the Fourth Amendment. Based on our review of the classified record, we agree that the applicable targeting and minimization procedures, which were followed in practice, sufficiently protected Mohamud’s privacy interest.

The government also contends that certain oversight procedures provide an important check on Executive Branch actions. For example, § 702 requires the Attorney General (“AG”) and Director of National Intelligence (“DNI”) to certify, among other things, that (1) a significant purpose of

the acquisition is to obtain foreign intelligence information, (2) they have adopted guidelines to ensure compliance with the statutory limitations in § 702(b), and (3) the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment. 50 U.S.C § 1881a(g)(2)(A); *see also id.* § 1881a(g)(1)(B) (providing that if the AG and DNI determine that “time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a)” they shall submit the certification “as soon as practicable but in no event later than 7 days after such determination is made”). Further, the AG and DNI must periodically assess whether the government is complying with FISC-approved targeting and minimization procedures and guidelines, which adds further oversight and privacy protections. *See* 50 U.S.C. § 1881a(i).

While Executive Branch certification contributes some degree of further protection, it does not weigh heavily. Typically in the Fourth Amendment context, review from a neutral magistrate is considered the appropriate check on the Executive, which otherwise may be motivated by its interest in carrying out its duties. *See, e.g., Leon*, 468 U.S. at 913–14 (explaining that in obtaining a search warrant, a neutral magistrate is “a more reliable safeguard against improper searches than the hurried judgment of a law enforcement officer ‘engaged in the often competitive enterprise of ferreting out crime’” (citation omitted)). Under these circumstances, where the only judicial review comes in the form of the FISC reviewing the adequacy of procedures, this type of internal oversight does not provide a robust safeguard. The government notes that in *In re Sealed Case*, 310 F.3d 717, 739 (FISA Ct. Rev. 2002), the FISA Review Court observed that Congress recognized that certification by the AG in the traditional FISA context would “‘assure [] written

accountability within the Executive Branch’ and provide ‘an internal check on Executive Branch arbitrariness.’” (citation omitted). However, as described above, § 702 differs in important ways from traditional FISA, and a mechanism that might provide additional protections above and beyond those already employed in a traditional FISA context provides far less assurance and accountability in the § 702 context, which lacks those baseline protections. *See also Clapper*, 133 S. Ct. at 1144–45.

Accordingly, although we do not place great weight on the oversight procedures, under the totality of the circumstances, we conclude that the applied targeting and minimization procedures adequately protected Mohamud’s diminished privacy interest, in light of the government’s compelling interest in national security.

In sum, even assuming Mohamud had a Fourth Amendment right in the incidentally collected communications, the search was reasonable. Thus, we hold that the application of § 702 did not violate the Fourth Amendment under the particular facts of this case.²⁸

²⁸ We also agree with the district court that the FISC survives separation of powers and non-delegation challenges, as FISC review of § 702 surveillance applications does not “interfere[] with the prerogatives of another branch of government beyond requiring the executive branch to conform to the statute,” and is “central to the mission of the judiciary” as it is similar to “the review of search warrants and wiretap applications.” *See Mistretta v. United States*, 488 U.S. 361, 388 (1989). Further, we agree with the district court that FISC opinions are not advisory because the FISC either approves or denies the requested acquisition (and electronic communication service providers must follow the directives or challenge them). *See* 50 U.S.C. § 1881a(h), (i)(2). Finally, the district court correctly rejected Mohamud’s First Amendment challenge, as motions to suppress based on First Amendment violations are analyzed

IV. CONCLUSION

Many young people think and say alarming things that they later disavow, and we will never know if Mohamud—a young man with promise—would have carried out a mass attack absent the FBI’s involvement. But some “promising” young people—Charles Whitman, Timothy McVeigh, and James Holmes, to name a few from a tragically long list—take the next step, leading to horrific consequences. While technology makes it easier to capture the thoughts of these individuals, it also makes it easier for them to commit terrible crimes. Here, the evidence supported the jury’s verdict, and the government’s surveillance, investigation, and prosecution of Mohamud were consistent with constitutional and statutory requirements.

AFFIRMED.

under the Fourth Amendment. *See, e.g., United States v. Mayer*, 503 F.3d 740, 747 (9th Cir. 2007) (where a party alleges that a criminal investigation violated the First Amendment rights of a third party, “we have held that the *Fourth Amendment* provides the relevant benchmark” (emphasis in original)); *United States v. Aguilar*, 883 F.2d 662, 697 (9th Cir. 1989).

NOT FOR PUBLICATION

FILED

UNITED STATES COURT OF APPEALS

DEC 05 2016

FOR THE NINTH CIRCUIT

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MOHAMED OSMAN MOHAMUD,

Defendant-Appellant.

No. 14-30217

D.C. No. 3:10-cr-00475-KI-1

MEMORANDUM*

Appeal from the United States District Court
for the District of Oregon
Garr M. King, District Judge, Presiding

Argued and Submitted July 6, 2016
Portland, Oregon

Before: PREGERSON, BEA, and OWENS, Circuit Judges.

Mohamed Osman Mohamud appeals from his jury conviction and thirty-year sentence for attempted use of a weapon of mass destruction within the United States, in violation of 18 U.S.C. § 2332a(a)(2)(A). As the parties are familiar with the facts, we do not recount them here. We have jurisdiction under 28 U.S.C.

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

§ 1291, and we affirm.¹

1. Mohamud challenges the government’s closing argument. Specifically, Mohamud contends that the government treated the entrapment defense as categorically unavailable by arguing that, based on the jury’s own “common sense,” an individual could not be entrapped to commit the charged offense. There was nothing improper about the government arguing that entrapment was unsupported by the facts because common sense suggested that someone could not be induced to commit a crime of this magnitude. The government did not imply that entrapment was unavailable as a matter of law.

Mohamud also contends that the government misstated the law, and diluted its burden of proof, by implying that predisposition to commit “similar acts” sufficed to prove predisposition to commit the charged offense. Although “evidence that merely indicates a generic inclination to act within a broad range . . . is of little probative value in establishing predisposition,” *Jacobson v. United States*, 503 U.S. 540, 550 (1992), evidence of prior similar acts may be relevant to show predisposition. See *United States v. Williams*, 547 F.3d 1187, 1198 (9th Cir. 2008) (holding that the defendant was not entrapped as a matter of law into dealing

¹ A concurrently filed opinion, *United States v. Mohamud*, __ F.3d __ (9th Cir. 2016), addresses Mohamud’s other arguments.

cocaine in part because his prior bank robbery and illegal gun sales “suggest[ed] that he was predisposed to this type of criminal activity”). Therefore, it was not improper for the government to argue that the jury could consider evidence of Mohamud’s willingness to commit prior similar acts.

2. Contrary to Mohamud’s contention, the district court provided adequate jury instructions. The instructions were consistent with case law and sufficiently encompassed the defense’s theory of the case. *See United States v. Whittemore*, 776 F.3d 1074, 1078, 1080 (9th Cir. 2015) (Although “[a] defendant is entitled to have the judge instruct the jury on his theory of defense, provided that it is supported by law and has some foundation in the evidence,” he is “not entitled to the instructions of his choice.” (citation omitted)). The district court also did not err in its response to a jury question about the entrapment instruction. *See United States v. Verduzco*, 373 F.3d 1022, 1030 n.3 (9th Cir. 2004) (setting forth standard of review). The response instructed the jury to consider “all” the evidence, and did not unfairly favor the prosecution’s evidence over the defense’s evidence.

3. Mohamud challenges the withholding and handling of classified materials under the Classified Information Procedures Act (“CIPA”), 18 U.S.C. app. 3. After reviewing the classified record, we are not persuaded by Mohamud’s arguments regarding the classified materials.

The district court acted within its discretion in excluding information about the true identities of FBI undercover agents “Youssef” and “Hussein” and FBI undercover contractor “Bill Smith.” *See United States v. Gil*, 58 F.3d 1414, 1421 (9th Cir. 1995) (explaining that a court “must weigh the defendants’ rights to confront the government’s witnesses against the government’s interest in not compromising investigations and in protecting the informant’s identity” (citing *Roviaro v. United States*, 353 U.S. 53, 60-62 (1957))). The district court also acted within its discretion in declining to make “Bill Smith” available as a witness at trial. *See id.*

In addition, the challenged substitution adequately satisfied CIPA’s requirement that the summary “provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information.” 18 U.S.C. app. 3, § 6(c)(1); *see also id.* § 4. The classified record does not support that the government “selectively declassified” materials, thereby gaining an unfair advantage at trial. The classified record also does not support that discoverable information which was “relevant and helpful” to the defense was withheld, including information regarding Amro Al-Ali. *United States v. Sedaghaty*, 728 F.3d 885, 904 (9th Cir. 2013) (quoting *Roviaro*, 353 U.S. at 60-61).

Further, the district court did not abuse its discretion by using ex parte proceedings for classified materials and denying Mohamud's security-cleared counsel access to classified materials and proceedings. *See id.* at 908-09 (rejecting the defendant's challenge to ex parte CIPA procedures and stating that "the simple fact that defense counsel held security clearances does not mean that the attorneys were entitled to access the government's classified filings").

4. Mohamud challenges a number of the district court's evidentiary rulings. Although the district court likely did make several erroneous evidentiary rulings, any error was cumulatively harmless.

First, Mohamud contends that the district court erred in admitting an Interpol "Red Notice" seeking the arrest of Amro Al-Ali. *See* Gov't Exhibit 80. He similarly argues that it was error to admit various FBI agents' testimony explaining how their knowledge of the Red Notice and Al-Ali's status affected their targeting and investigation of Mohamud. Generally, evidence of agents' motivations or justifications for an investigation are irrelevant, even where entrapment is at issue. *See United States v. Makhlouta*, 790 F.2d 1400, 1402 (9th Cir. 1986) (explaining that under the entrapment standard, "it is not the state of mind of the government agent that is important; . . . it is the predisposition of the defendant . . . that counts" (first alteration in original) (citation and internal quotation marks omitted)); *see*

also *United States v. Dean*, 980 F.2d 1286, 1288 (9th Cir. 1992) (out-of-court statements which were probative of why officer took certain actions were inadmissible because they did “not bear on any issue involving the elements of the charged offense”). However, as the defense argued that the government targeted Mohamud because he was young and vulnerable, evidence that the government instead investigated him because of his communications with a “known terrorist” was relevant under Federal Rule of Evidence 401.² Nonetheless, only the testimony of the agents who actually directed the investigation was relevant to rebut Mohamud’s “targeting” arguments; the comparable testimony of the undercover agents was not relevant, nor was the Red Notice itself.³ Further, in several instances the government used this evidence for the truth of the matter asserted, rather than its effect on the agents.

Second, Mohamud argues that the district court erroneously restricted his cross-examination of the FBI agents’ bias and motivation by treating inadvertently recorded government agent “outtakes” as prior inconsistent statements under

² “Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.” Fed. R. Evid. 401.

³ Because the Red Notice was admitted for a non-hearsay use, it did not violate Mohamud’s right to confrontation. See *United States v. Wahchumwah*, 710 F.3d 862, 871 (9th Cir. 2012).

Federal Rule of Evidence 613. It is not clear that the court abused its discretion in so ruling, no error was by itself prejudicial, and any such errors were not cumulatively prejudicial. Mohamud was permitted to question the agents about the statements, and the only evidence excluded was the agents' tone of voice on the recording.

Third, Mohamud contends that the district court erred in permitting government witnesses to testify about what they believed Mohamud "meant" or was "thinking" in some of his recorded statements. We agree that the witnesses' speculation as to what Mohamud "meant" was not relevant under Rule 401.

Finally, Mohamud argues that the district court erred in excluding certain of his contemporaneous communications that reflected a lack of predisposition to commit the crime charged.⁴ Such statements were admissible under Federal Rule of Evidence 803(3) as indicative of Mohamud's then-existing state of mind, and it was likely error to exclude them. The government's cited authority is not to the contrary. *Cf. United States v. Sayakhom*, 186 F.3d 928, 937 (9th Cir.), *amended by* 197 F.3d 959 (9th Cir. 1999) (holding that the defendant's statements were not admissible because they were statements of belief to prove the fact believed, which

⁴ Mohamud was permitted to introduce some evidence of his contemporaneous state of mind, but some statements were excluded.

are inadmissible under the terms of Rule 803(3)).

With respect to cumulative error, “[t]here are some cases where the cumulative effect of multiple errors may so prejudice a defendant as to require reversal, even though no single trial error examined in isolation is sufficiently prejudicial to warrant reversal.” *United States v. Cazares*, 788 F.3d 956, 990 (9th Cir. 2015). We consider here any error related to: (1) admitting the Red Notice and the undercover agents’ related testimony,⁵ and any improper hearsay use of the Red Notice; (2) excluding the recorded government agent “outtakes”; (3) allowing the agents to speculate about what Mohamud meant in certain recorded statements; and (4) excluding some of Mohamud’s contemporaneous statements.

As a preliminary matter, the government failed to argue that the evidentiary errors were harmless, except with respect to the exclusion of Mohamud’s contemporaneous statements. “Usually when the government fails to argue harmlessness, we deem the issue waived and do not consider the harmlessness of any errors we find.” *United States v. Gonzalez-Flores*, 418 F.3d 1093, 1100 (9th Cir. 2005). However, we have discretion “to consider harmlessness sua sponte in extraordinary cases.” *United States v. Brooks*, 772 F.3d 1161, 1171 (9th Cir.

⁵ The district court gave several limiting instructions that this evidence was relevant only for its effect on the agents’ understanding (“mental state”).

2014). In doing so, we must consider “(1) the length and complexity of the record, (2) whether the harmlessness of an error is certain or debatable, and (3) the futility and costliness of reversal and further litigation.” *Id.* (quoting *Gonzalez-Flores*, 418 F.3d at 1101). The second factor is the most important. *Id.*

Here, in the context of the entire trial record, “the harmlessness of the error[s] is not reasonably debatable,” and further litigation would be futile. *Gonzalez-Flores*, 418 F.3d at 1101. Accordingly, we hold that any evidentiary errors were cumulatively harmless.

5. The district court denied Mohamud’s motion to suppress, in which he argued that the FBI’s conduct related to a separate state police investigation was unconstitutional, and therefore later national security investigation evidence was the fruit of an illegal search. The district court reasoned that the later national security investigation evidence was based on untainted, independent sources. Contrary to Mohamud’s contention, the district court did not err by declining to determine whether the FBI’s conduct violated Mohamud’s constitutional rights. *See United States v. Crawford*, 372 F.3d 1048, 1053-54 (9th Cir. 2004) (en banc) (affirming denial of motion to suppress on attenuation grounds, and stating that the court “need not” decide whether the search violated the defendant’s Fourth Amendment rights).

6. The district court did not abuse its discretion by denying Mohamud's security-cleared counsel access to classified materials under the Foreign Intelligence Surveillance Act of 1978 ("FISA"). *See* 50 U.S.C. § 1806(f) (providing that under FISA, "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"); *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987) (holding that FISA's ex parte in camera proceedings did not violate due process, even though defense counsel had high security clearances).⁶ In addition, and as stated above, the summary of classified materials provided by the FBI adequately satisfied CIPA's requirement that the summary "provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information." 18 U.S.C. app. 3, § 6(c)(1); *see also id.* § 4.

7. Finally, Mohamud argues that we should vacate his thirty-year sentence for two reasons, neither of which we find persuasive. First, we reject Mohamud's

⁶ On appeal, Mohamud alternatively requested that we authorize supplemental briefing with defense access to the relevant classified FISA materials. We granted this request in part because, at our request post-argument, the government declassified certain facts about Mohamud's surveillance, and we permitted the parties to file supplemental briefs.

contention that his sentence should be vacated because the government's forty-year sentencing recommendation was allegedly based in part on unlawful considerations.

Second, Mohamud contends that the district court procedurally erred by failing to resolve his future dangerousness on an individualized basis and by failing to explain adequately its reasons for rejecting a departure from the terrorism criminal history enhancement under U.S.S.G. § 4A1.3. These contentions are belied by the record. The district court considered Mohamud's arguments and evidence about his purported lack of future dangerousness, weighed individualized mitigating and aggravating factors, and adequately explained its reasons for Mohamud's below-Guidelines thirty-year sentence. *See United States v. Sandoval-Orellana*, 714 F.3d 1174, 1181 (9th Cir. 2013) ("If the record 'makes clear that the sentencing judge listened to each argument' and 'considered the supporting evidence,' the district court's statement of reasons for the sentence, although brief, will be 'legally sufficient.'" (quoting *Rita v. United States*, 551 U.S. 338, 358 (2007))).

AFFIRMED.

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,

Criminal Case No. 3:10-CR-00475-KI-1

Plaintiff,

OPINION AND ORDER

v.

MOHAMED OSMAN MOHAMUD,

Defendant.

S. Amanda Marshall
United States Attorney
District of Oregon
Ethan D. Knight
Pamala R. Holsinger
United States Attorney's Office
1000 S.W. Third Avenue, Suite 600
Portland, Oregon 97204
John P. Carlin
George Z. Toscas
J. Bradford Wiegmann
Tashina Gauhar
Jolie F. Zimmerman

National Security Division
United States Department of Justice

Attorneys for Plaintiff

Steven T. Wax
Federal Public Defender
Stephen R. Sady
Lisa Hay
Office of the Federal Public Defender
101 SW Main Street, Suite 1700
Portland, Oregon 97204

Attorneys for Defendant

KING, Judge:

The Foreign Intelligence Surveillance Court of Review (“FISA Court of Review”) has explained the difficult exercise which I now undertake:

Our government is tasked with protecting an interest of utmost significance to the nation—the safety and security of its people. But the Constitution is the cornerstone of our freedoms, and government cannot unilaterally sacrifice constitutional rights on the altar of national security. Thus, in carrying out its national security mission, the government must simultaneously fulfill its constitutional responsibility to provide reasonable protections for the privacy of United States persons. The judiciary’s duty is to hold that delicate balance steady and true.

In re Directives [Redacted] Pursuant to Section 105B of FISA, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

Title I and Title III of the Foreign Intelligence Surveillance Act of 1978 (“FISA”), 50 U.S.C. §§ 1801-1812, 1821-1829, allow electronic surveillance and physical search after obtaining a FISA warrant from the Foreign Intelligence Surveillance Court (“FISC”). The government provided a FISA notification to defendant at his first appearance, advising him it intended to use evidence

PAGE 2 - OPINION AND ORDER

obtained under Title I and Title III. Defendant unsuccessfully relied on an entrapment defense. A jury convicted him in January 2013 of attempting to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(A).

Section 702 of the FISA Amendments Act of 2008 (“FAA”), 50 U.S.C. § 1881a (part of Title VII of FISA, which is codified at §§ 1881a-1881g), permits, subject to statutory requirements, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information.

Unlike traditional FISA surveillance, § 1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. And, unlike traditional FISA, § 1881a does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.

....

Section 1881a mandates that the Government obtain the Foreign Intelligence Surveillance Court’s approval of “targeting” procedures, “minimization” procedures, and a governmental certification regarding proposed surveillance.

Clapper v. Amnesty Int’l USA, 133 S. Ct. 1138, 1144-45 (2013) (internal citations omitted).

On November 19, 2013, the government filed a Supplemental FISA Notification:

This supplemental notice is being filed as a result of the government’s determination that information obtained or derived from Title I FISA collection may, in particular cases, also be “derived from” prior Title VII FISA collection. Based upon that determination and a recent review of the proceedings in this case, the United States hereby provides notice to this Court and the defense, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the government has offered into evidence or otherwise used or disclosed in proceedings, including at trial, in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.

Defendant intended to challenge the constitutionality of Title VII and claimed he needed broad discovery to provide the court with the full factual context surrounding the legal issues relevant to the newly-noticed surveillance. On March 19, 2014, I denied defendant's motion seeking this discovery. Now before the court are defendant's Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the Pretrial Notice Statute [500], defendant's Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance [502], and defendant's Second Motion for a New Trial [504]. Generally speaking, defendant seeks suppression of evidence obtained or derived through § 702 or fruits of that evidence, as well as other related or alternative relief. I deny the motions for the reasons I explain below. I am also filing an accompanying classified opinion to explain some of my reasoning.

DISCUSSION

I. Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the Pretrial Notice Statute

Under 50 U.S.C. § 1881e(a), information acquired under § 702 is deemed information acquired from an electronic surveillance and is subject to the notice requirement in 50 U.S.C. § 1806(c). Defendant argues the government violated the notice statute by failing to provide notice of § 702 surveillance in the original pretrial FISA notification. As a remedy, defendant seeks dismissal of the indictment or a new trial after suppression of evidence.

Defendant first objects to what he contends are contradictory statements in the government's briefing for the discovery motion I just denied. Defendant sees a contradiction between: (1) the government's statement that it had not previously considered if evidence obtained through electronic surveillance under Title I/III could also be considered as a matter of law to be derived from a prior collection under Title VII and; (2) the government's statement that the prosecutors acted in accordance with the then-current standard practice.

The government explains it provided the Supplemental Notification after deciding evidence obtained under Title I/III could also be considered to be derived from prior collection under Title VII as a matter of law. A changed legal opinion is a different issue from following the standard practice up to that point. I do not see the contradiction troubling defendant.

Next, defendant claims he has established a prima facie case regarding the circumstances surrounding the statutory violation, relying on speculation and public disclosures about Clapper. He argues that to rebut this prima facie case, the government must file affidavits to support its explanation concerning the reason it filed the Supplemental Notification. This is not a situation, however, where the law supports presumptions based on a prima facie case.¹

I now turn to the legal arguments defendant brings forward, the first of which is based on cases in effect when Congress enacted FISA. Because the FISA notice provision requires notice to both the aggrieved person and the court, defendant argues dismissal of the indictment or a new trial provide the only mechanisms to vindicate the separation of powers doctrine and to effectuate the choice the Supreme Court has imposed on the government. Defendant relies on a trilogy of Supreme

¹ I am unpersuaded the burden-shifting analysis for resolving summary judgment motions in employment discrimination cases, as set forth in McDonnell Douglas Corp. v. Green, 411 U.S. 792 (1981), and cited by defendant, has any application to the issue before me.

Court cases requiring the government to choose between disclosure and dismissal of the indictment: Jencks v. United States, 353 U.S. 657, 672, 77 S. Ct. 1007 (1957) (defendant was entitled to reports of government witnesses testifying at trial; the criminal action must be dismissed if the government, on the ground of privilege, elects not to comply with an order to produce), Roviaro v. United States, 353 U.S. 53, 61, 77 S. Ct. 623 (1957) (if an informer's identity is relevant and helpful to the defense or is essential to a fair trial, the government must disclose the identity or dismiss the indictment), and Alderman v. United States, 394 U.S. 165, 184, 89 S. Ct. 961 (1969) (in the context of electronic surveillance with no statutory notice requirement, government must disclose surveillance records needed to determine the legality of the surveillance or dismiss the indictment). Defendant contends these cases provide a framework for protection of the separation of powers because they enforce legislative and judicial constraints on executive over-reaching in prosecution.

The government's response is based on FISA's provision under 50 U.S.C. § 1806(e) which allows defendant to move to suppress evidence unlawfully acquired. Because this remedy would put defendant in a similar position to the government having provided the Supplemental Notification before trial, the government argues dismissal of the indictment is unnecessary. The government contends defendant's trilogy of Supreme Court cases do not apply to his situation because, here, the government did not affirmatively withhold disclosure of the use of the Title VII-derived evidence in defiance of a court order.

Congress was aware of Jencks, Roviaro, and Alderman when it enacted FISA, yet it chose to provide the single remedy of suppression, not dismissal of the indictment, when the government unlawfully acquired evidence under the statute. Defendant has argued no persuasive reason to limit the term "unlawfully acquired . . . under the statute" to exclude a failure to provide the statutory

PAGE 6 - OPINION AND ORDER

notice. In addition, as the government notes, FISA even anticipates a suppression motion may be filed after trial: “Such a motion shall be made before the trial . . . unless . . . the person was not aware of the grounds of the motion.” 50 U.S.C. § 1806(c). If Congress wished to provide a harsher penalty for a notification violation, it could have done so.

Alternatively, defendant claims the court can dismiss the indictment or grant a new trial to remedy the government’s intentional or reckless violation of the FISA notice provision, based on an exercise of the court’s inherent supervisory power, Federal Rule of Criminal Procedure 16(d), and Brady authority. Even if the government did not intentionally violate the notice provision, defendant claims the government’s reckless disregard for the statutory obligation warrants dismissal.

The government argues dismissing the indictment would serve no valid purpose because there was no constitutional violation. Because FISA provides an appropriate remedy, the government contends defendant cannot show substantial prejudice, and the court may take less severe action than dismissal. The government claims there was no prosecutorial misconduct, much less flagrant misconduct, when it provided notice under the standard practice at the time. Once the government changed its legal opinion, it provided the Supplemental Notification which allowed defendant to file the pending motion to suppress. Further, the government argues there were no discovery violations and there is no new evidence, making sanctions under Rule 16 or Brady inappropriate.

I agree with defendant that I have the power to dismiss the indictment under my inherent supervisory powers and for violations of the discovery obligations under the Constitution and federal rules. See United States v. Chapman, 524 F.3d 1073, 1084-88 (9th Cir. 2008) (under its supervisory power, the court may dismiss an indictment for flagrant prosecutorial misconduct, which can include

PAGE 7 - OPINION AND ORDER

reckless disregard for the prosecution's constitutional obligations under Brady and Giglio); United States v. Hernandez-Meza, 720 F.3d 760, 769 (9th Cir. 2013) (indictment can be dismissed for willful Rule 16 violation). But dismissal is not warranted here.

The court may exercise its supervisory power "to remedy a constitutional or statutory violation; to protect judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; or to deter future illegal conduct." United States v. Stinson, 647 F.3d 1196, 1210 (9th Cir. 2011) (internal quotations omitted), cert. denied, 132 S. Ct. 1768 (2012). Dismissal is available "when the investigatory or prosecutorial process has violated a federal constitutional or statutory right and no lesser remedial action is available." United States v. Barrera-Moreno, 951 F.2d 1089, 1092 (9th Cir. 1991).

As explained above, FISA provides a lesser remedy if necessary—suppression. Thus, the harsh remedy of dismissal is not needed. Clearly a lot of time has passed, but otherwise suppression and a new trial would put defendant in the same position he would have been in if the government notified him of the § 702 surveillance at the start of the case. Moreover, the government has apparently changed its practice in making this type of notification, so dismissal is not needed as a deterrence.

In addition, once the government changed its legal opinion about when evidence could be derived under Title VII, it performed the second review of this case and provided the Supplemental Notification without prodding from the court or the defense. If the government had kept mum about the situation in this case, I would have sentenced defendant months ago. I consider this strong evidence of the lack of prosecutorial misconduct.

For these reasons, I deny defendant's motion for vacation of conviction and alternative remedies of dismissal of the indictment, suppression of evidence, and new trial for the government's violation of the pretrial notice statute.

II. Second Motion for a New Trial

Defendant went to trial to present an entrapment defense. He argued he was not predisposed to attempt to use a weapon of mass destruction in the United States, and he was induced into doing so. He divides the withheld evidence into three parts: (1) the fact of additional surveillance; (2) the scope of that surveillance; and (3) the evidence generated by that surveillance. Defendant is at a grave disadvantage in articulating how the withheld evidence might have affected the trial, because he has not seen it, but he presents a few scenarios he considers likely.

According to defendant, if he had the withheld evidence before trial, he could have argued that the lack of evidence of predisposition, in light of the additional and pervasive surveillance, more strongly suggests he was not predisposed. With respect to inducement, defendant could have argued the knowledge the government gained through the additional surveillance allowed the government to more closely tailor the sting operation. Defendant claims the jury should have seen the withheld evidence to fully assess the government's conduct. Thus, defendant considers the late notification of the Title VII surveillance a Brady violation, as well as a violation of his other fundamental constitutional rights guaranteeing a fair trial, and he seeks a new trial as a remedy.

The government assumes defendant is moving for a new trial under Federal Rule of Criminal Procedure 33, which allows the court to grant a new trial if the interest of justice so requires or if there is newly discovered evidence. The government reminds us the Supplemental Notification referred to evidence previously addressed before trial that was derived from a Title VII collection as

well as being obtained in a Title I/III collection. Thus, the government argues there is no new evidence, and defendant's inference that the surveillance was pervasive in scope is only an inference, not new evidence. Moreover, the government claims the specific information at issue would not have been helpful to the defense or resulted in acquittal, as detailed in the government's classified brief. The government contends it presented overwhelming evidence of defendant's guilt at trial, and notes the jury convicted defendant even after the defense argued the pervasive scope of government surveillance to the jury.

Because defendant makes broad arguments, I will state a few standards which could apply. A party seeking a trial on newly discovered evidence must prove:

(1) the evidence is newly discovered; (2) the defendant was diligent in seeking the evidence; (3) the evidence is material to the issues at trial; (4) the evidence is not (a) cumulative or (b) merely impeaching; and (5) the evidence indicates the defendant would probably be acquitted in a new trial.

United States v. Hinkson, 585 F.3d 1247, 1265 (9th Cir. 2009), reh'g denied and dissenting op. vacated and superseded, 611 F.3d 1098 (9th Cir. 2010).

For the court to grant a new trial because of a Brady violation, it must determine that the documents, if favorable to the defendant, "undermine its confidence in the outcome and that there is a reasonable probability of a different result." United States v. Doe, 705 F.3d 1134, 1152-53 (9th Cir. 2013) (internal quotation omitted).

Although defendant vehemently disagrees, the fundamental problem with defendant's argument is that there is no new evidence. A surveillance is not evidence—it produces evidence. Even with an entrapment defense, the way in which the government was able to tailor the sting operation is not relevant to entrapment. What is relevant to entrapment are the actual contacts

between government agents and the defendant. Those contacts were presented in detail to the jury, including hours of video and audio recordings. The jury was able to fully assess the government's conduct, as was I. The defense brought forward the pervasiveness of the surveillance of defendant, even lacking knowledge of the § 702 surveillance referenced in the Supplemental Notification. Moreover, even if there were a Brady violation, I cannot say my confidence in the outcome of the trial is undermined or that there is a reasonable probability of a different result.

Defendant further argues the government presented its investigation as being above reproach. He speculates that depending on the content of the withheld evidence, the defense might have been able to impeach government witnesses' characterizations of the investigation and thereby cast doubt on their credibility.

The government claims that even if the fact of the § 702 collection would impeach a government witness, new impeachment evidence does not support a motion for a new trial except in extraordinary circumstances.

As stated above in the factors for a new trial under Hinkson, impeachment evidence is usually not enough to support a request for a new trial. However, there is one exception:

[T]he newly-discovered impeachment evidence may be so powerful that, if it were to be believed by the trier of fact, it could render the witness' testimony totally incredible. In such a case, if the witness' testimony were uncorroborated and provided the only evidence of an essential element of the government's case, the impeachment evidence would be "material" under [United States v. Walgren, 885 F.2d 1417, 1428 (9th Cir.1989)]. Moreover, Rule 33 permits the granting of a new trial motion "if required in the interest of justice." Fed. R. Crim. P. 33. If newly-discovered evidence establishes that a defendant in a narcotics case has been convicted solely on the uncorroborated testimony of a crooked cop involved in stealing drug money, the "interest of justice" would support a new trial under Rule 33.

United States v. Davis, 960 F.2d 820, 825 (9th Cir. 1991).

That is clearly not the situation here. Introduction of the fact of the § 702 surveillance referenced in the Supplemental Notification would not gut the government's case against defendant.

Accordingly, I deny defendant's second motion for a new trial.

III. Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance

A. Overview of FISA

I first provide an overview of FISA's history and an explanation of some of its provisions:

As originally enacted in 1978, FISA generally requires a warrant to conduct electronic surveillance, as that term was defined in the Act. 50 U.S.C. § 1809(a)(1). Congress precisely defined electronic surveillance to cover four types of domestic foreign intelligence collection activities, with the type being dependent, in part, on whether a wire or a radio communication is being acquired. 50 U.S.C. § 1801(f). Based on witness testimony, Congress understood that most foreign-to-foreign and international communications were outside FISA's proposed definition of electronic surveillance.

“[T]he language of this amendment exempts . . . foreign intelligence gathering from international or foreign communications by means of an electronic, mechanical, or other surveillance device if the acquisition does not come within the definition of “electronic surveillance” Specifically this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.

See S. Rep. No. 95-701, at 71 (1978).

According to the government, if a particular known U.S. person in the United States was not intentionally targeted, FISA, when first enacted, “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." Government's Unclassified Resp. to Def.'s Alternative Mot. for Suppression of Evidence and a New Trial 11, ECF No. 500 [hereinafter Govt.'s Brief]. Communications technology changed dramatically as the decades passed, causing unforeseen consequences under FISA.

More specifically, the DNI [Director of National Intelligence] explained that, whereas international communications were predominantly carried by radio when FISA was enacted, that was no longer true: "Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally by fiber optic cables"—and therefore qualify as wire communications under FISA. [Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intel., 110th Cong. 1st Sess. (May 1, 2007), at 19. ("May 1, 2007 FISA Modernization Hrg.")]. Thus, many international communications that would have been generally excluded from FISA regulation in 1978, when they were carried by radio, were now potentially included, due merely to a change in technology rather than any intentional decision by Congress. Id.

Further, the DNI stated, with respect to the collection of wire communications, FISA's "electronic surveillance" definition "places a premium on the location of the collection." May 1, 2007 FISA Modernization Hrg. at 19; see 50 U.S.C. § 1801(f)(2). The DNI explained that technological advances had rendered this distinction outmoded as well: "Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart." May 1, 2007 FISA Modernization Hrg. at 19.

Govt.'s Brief 13-14 (footnote omitted).

To update FISA, Congress enacted the Protect America Act ("PAA") in August 2007; under a sunset provision, it expired in February 2008. In July 2008, Congress enacted the FISA Amendments Act of 2008 ("FAA"), including § 702, the center of the dispute in this motion. Under § 702, after the FISC issues an order, the Attorney General and the DNI "may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably

PAGE 13 - OPINION AND ORDER

believed to be located outside the United States to acquire foreign intelligence information.” 50 U.S.C. § 1881a(a).

Section 702 includes limitations to protect domestic communications. An acquisition:

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) 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; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

50 U.S.C. § 1881a(b).

Minimization procedures “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.”

50 U.S.C. § 1801(h)(1).

If the FISC approves the targeting and minimization procedures and the certification from the Attorney General and DNI, it will approve the acquisition. Under 50 U.S.C. § 1881a(g)(2)(A), the certification must attest:

(1) there are procedures in place that have been approved, submitted for approval, or will be submitted with the certification for approval by the FISC that are reasonably designed to ensure that an acquisition (a) is limited to targeting persons reasonably believed to be located outside the United States and (b) to prevent the intentional acquisition of any communication in which the sender and all intended recipients are known to be located in the United States;

(2) the minimization procedures meet the definition of minimization procedures under Title I/III and have been approved, submitted for approval, or will be submitted with the certification for approval by the FISC;

(3) the Attorney General has adopted guidelines to ensure compliance with the limitations in 50 U.S.C. § 1881a(b) [quoted above];

(4) the procedures and guidelines are consistent with the requirements of 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 50 U.S.C. § 1881a(b) [quoted above];

In addition, the certification must include copies of the targeting and minimization procedures, a supporting affidavit from an appropriate national security official, and an effective date. 50 U.S.C. § 1881a(g)(2)(B)-(D). The FISC can approve the certification and related targeting and minimization procedures, or it can direct the government to either (1) correct any deficiency within 30 days or (2) cease or not begin implementation of the authorization. 50 U.S.C. § 1881a(i)(3)(B).

Section 702 allows the government to compel an electronic communication service provider to acquire the authorized communications. 50 U.S.C. § 1881a(h). The National Security Agency (“NSA”) “provides specific identifiers (for example, e-mail addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification.” The National Security Agency: Missions, Authorities, Oversight and Partnerships 4, available at http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf (Aug. 9, 2013).

B. Separation of Powers

As a threshold issue, defendant claims § 702 violates the separation of powers doctrine. The Fourth Amendment inserts a neutral and detached magistrate between the subject of the search and the government. Defendant claims § 702 procedures reduce the role of the judge to consulting with the Executive Branch with no case or controversy involving an adversary. He contends the FISC does not approve or disapprove proposals for § 702 surveillance but instead has a role in designing them. Defendant characterizes the FISC’s role as providing a non-judicial advisory opinion, and he argues this violates the fundamental separation of powers function of the Warrant Clause.

The government disagrees and analogizes the FISC role to numerous judicial functions not directly connected to adversarial proceedings.

The FISA Court of Review has noted it does “not think there is much left to an argument made by an opponent of FISA in 1978 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 Sealed Case, 310 F.3d 717, 732 n.19 (FISA Ct. Rev. 2002)

(citing Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, 9745, 7308, and 5632 Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence, 95th Cong., 2d Sess. 221 (1978) (statement of Laurence H. Silberman)). I agree.

The Supreme Court has approved numerous congressional delegations of power which did not upset the balance of power established in the Constitution:

The nondelegation doctrine is rooted in the principle of separation of powers that underlies our tripartite system of Government. The Constitution provides that “[a]ll legislative Powers herein granted shall be vested in a Congress of the United States,” U.S. Const., Art. I, § 1, and we long have insisted that “the integrity and maintenance of the system of government ordained by the Constitution” mandate that Congress generally cannot delegate its legislative power to another Branch. Field v. Clark, 143 U.S. 649, 692, 12 S. Ct. 495, 504, 36 L. Ed. 294 (1892). We also have recognized, however, that the separation-of-powers principle, and the nondelegation doctrine in particular, do not prevent Congress from obtaining the assistance of its coordinate Branches. . . . So long as Congress “shall lay down by legislative act an intelligible principle to which the person or body authorized to [exercise the delegated authority] is directed to conform, such legislative action is not a forbidden delegation of legislative power.” J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409, 48 S. Ct. 348, 352 (1928).

Mistretta v. United States, 488 U.S. 361, 371-72, 109 S. Ct. 647 (1989) (holding Sentencing Guidelines are constitutional, Congress did not delegate excessive legislative power to the Commission and did not violate the separation-of-powers principle, judges traditionally determine sentences). “[C]onsistent with the separation of powers, Congress may delegate to the Judicial Branch nonadjudicatory functions that do not trench upon the prerogatives of another Branch and that are appropriate to the central mission of the Judiciary.” Id. at 388.

The statutory scheme Congress specified for § 702 surveillance is sufficient to serve as the intelligible principle to which FISC judges must conform in reviewing applications. In particular, the FISC review must insure the surveillance will be conducted in a manner consistent with the

Fourth Amendment. 50 U.S.C. § 1881a(b)(5), (g)(2)(A)(4). The judiciary certainly is well-prepared to fulfill that function. Furthermore, determining if a statute is constitutional is not a prohibited executive or administrative duty which would violate the separation of powers doctrine. See Morrison v. Olson, 487 U.S. 654, 677, 108 S. Ct. 2597 (1988) (in upholding the constitutionality of the Ethics and Government Act under Article III and the separation of powers doctrine, the Court noted, “As a general rule, we have broadly stated that executive or administrative duties of a nonjudicial nature may not be imposed on judges holding office under Art. III of the Constitution.”) (internal quotation omitted).

Indeed, as the government points out, the judiciary also issues search warrants and reviews wiretap applications, both of which are ex parte proceedings. Id. at 389 n.16. I am not persuaded the review of § 702 surveillance applications interferes with the prerogatives of another branch of government beyond requiring the executive branch to conform to the statute. Review of § 702 surveillance applications is as central to the mission of the judiciary as the review of search warrants and wiretap applications.

Moreover, I disagree with defendant’s argument that the FISC judges only provide advisory opinions. The FISC judge reviews the certification, targeting procedures, and minimization procedures included in a § 702 surveillance application and either approves the acquisition or orders the government to choose between correcting deficiencies within 30 days and ceasing or not beginning the acquisition. 50 U.S.C. § 1881a(i)(2). Similarly, electronic communication service providers must follow directives to acquire communications or challenge the directive before the FISC; the opinions are not advisory. 50 U.S.C. § 1881a(h).

Although I am not a FISC judge, I disagree with defendant's argument that the FISC judges assist in designing § 702 procedures. FISC opinions now declassified inform us that the court meets with senior officials at the Department of Justice to discuss information provided in the submissions. [Caption Redacted], [docket no. redacted], 2011 WL 10945618, at *3 (FISA Ct. Oct. 3, 2011). The technology underlying the surveillance is so extremely complex there is likely little possibility of understanding it without question sessions like this. If the FISC disapproves a government submission, it explains why. The government can then make changes addressing the problems and resubmit the submission. This is the normal way courts operate—justice is not served if the court does not explain its decisions.

Finally, “[p]rior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.” United States v. United States Dist. Court for E. Dist. of Mich., 407 U.S. 297, 318, 92 S. Ct. 2125 (1972)(citing Beck v. Ohio, 379 U.S. 89, 96, 85 S. Ct. 223 (1964)) (in the criminal prosecution for the bombing of a CIA office in Michigan, warrantless wiretaps conducted as part of a domestic security surveillance violated the Fourth Amendment) [hereinafter Keith]. Although the FISC is not reviewing a warrant application under § 702, the FISC review of § 702 surveillance submissions provides prior review by a neutral and detached magistrate. This strengthens, not undermines, Fourth Amendment rights.

Accordingly, I conclude § 702 does not violate the separation of powers doctrine.

C. Constitutionality of Section 702 under the First Amendment

Defendant contends the breadth and vagueness of § 702 surveillance chill Americans' exercise of their First Amendment rights, causing many to change their habits in using the Internet

and telephones. Defendant claims this chill is sufficient to create a First Amendment violation, invalidating § 702.

The government responds that First Amendment interests in a criminal investigation are protected by the Fourth Amendment, and motions to suppress based on alleged First Amendment violations are analyzed under the Fourth Amendment and the exclusionary rule.

Defendant raises a significant point: “Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with scrupulous exactitude.” Zurcher v. Stanford Daily, 436 U.S. 547, 564, 98 S. Ct. 1970 (1978) (internal quotation omitted) (a search warrant for a newspaper which was not suspected of a crime does not violate the First Amendment because the warrant’s preconditions adequately safeguard the newspaper’s ability to gather and publish the news).

But the appropriate analysis is under the Fourth Amendment, not the First Amendment. United States v. Mayer, 503 F.3d 740, 747-48 (9th Cir. 2007) (affirming conviction based on investigation with FBI agent going undercover as a member of organization opposed to sexual age-of-consent laws, “First Amendment concerns become part of the Fourth Amendment analysis because, under the Fourth Amendment, the court must examine what is unreasonable in the light of the values of freedom of expression” (citing Roaden v. Kentucky, 413 U.S. 496, 504, 93 S. Ct. 2796 (1973))).

Defendant cites a concurrence in Nevada Commission on Ethics v. Carrigan for the proposition that a statute is invalid if it “operates to chill or suppress the exercise of First Amendment freedoms by reason of vague terms or overbroad coverage.” Nevada Commission on Ethics v. Carrigan, 131 S. Ct. 2343, 2353 (2011) (Kennedy, J., concurring) (state government

conflict of interest rule did not violate legislator's First Amendment rights). I have no quarrel with this blackletter statement of the law, but Nevada Commission on Ethics is far afield from § 702 surveillance.

Consequently, I will follow Mayer and move on to a Fourth Amendment analysis, but I will apply the Fourth Amendment requirements with "scrupulous exactitude," as required by Zurcher.

D. Constitutionality of Section 702 under the Fourth Amendment

The Fourth Amendment states:

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

"[N]either a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance." Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 665, 109 S. Ct. 1384 (1989) (suspicionless drug-testing of certain United States Custom Service employees was reasonable under Fourth Amendment).

The parties agree on one thing: 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, 110 S. Ct. 1056 (1990) (Fourth Amendment did not apply to American law enforcement's search of the Mexican residences of a Mexican citizen with no voluntary attachment to the United States). Section 702 is aimed at acquiring communications of non-U.S. persons outside the United States, and thus not entitled to Fourth Amendment protection. The dispute arises because communications of U.S. persons located in the United States can be incidentally acquired.

The government claims the § 702 acquisition targeting non-U.S. persons outside the United States is constitutional because: (1) the incidental collection of communications of U.S. persons does not trigger the warrant requirement; (2) surveillance authorized under § 702 falls within the foreign intelligence exception to the warrant requirement; and (3) surveillance authorized under § 702 is a reasonable search under the Fourth Amendment.

Defendant strongly disagrees:

[R]egardless of the nominal targeting of foreign persons abroad, the § 702 programs routinely acquire huge numbers of American communications in America . . . [which] implicate[] the Fourth Amendment. This case is a test of fundamental American liberties: the Court should reject the claim that, simply because foreign persons are being targeted, Americans lose their rights as collateral damage.

Def.'s Reply to Government's Unclassified Resp. to Def.'s Alternative Mot. for Suppression of Evidence 4, ECF No. 513 [hereinafter Def.'s Reply].

First, I must address whether defendant's challenge to § 702 must be limited to an "as applied" challenge, as the government argues, or also include a facial challenge, as defendant argues. Defendant relies on Berger v. State of New York, 388 U.S. 41, 87 S. Ct. 1873 (1967), in which the Court held a state statute, allowing law enforcement to obtain ex parte orders for eavesdropping, violated the Fourth Amendment because it was overbroad and allowed "a trespassory invasion of the home or office, by general warrant." Id. at 44, 64. The Court allowed the facial challenge, even though the defendant was convicted using evidence obtained by the eavesdropping order. Id. at 44. The Court took the opposite approach in Sibron v. New York, 392 U.S. 40, 59, 88 S. Ct. 1889 (1968) (refusing to undertake a facial challenge to the constitutionality of New York's stop-and-frisk law), and distinguished Berger:

PAGE 22 - OPINION AND ORDER

The parties on both sides of these two cases have urged that the principal issue before us is the constitutionality of § 180-a ‘on its face.’ We decline, however, to be drawn into what we view as the abstract and unproductive exercise of laying the extraordinarily elastic categories of § 180-a next to the categories of the Fourth Amendment in an effort to determine whether the two are in some sense compatible. The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case. In this respect it is quite different from the question of the adequacy of the procedural safeguards written into a statute which purports to authorize the issuance of search warrants in certain circumstances. See Berger. No search required to be made under a warrant is valid if the procedure for the issuance of the warrant is inadequate to ensure the sort of neutral contemplation by a magistrate of the grounds for the search and its proposed scope, which lies at the heart of the Fourth Amendment.

Sibron, 392 U.S. at 59 (internal citation omitted).

Defendant contends his facial challenge to § 702 concerns the adequacy of its procedural safeguards, and should be allowed under Berger.

The government insists the challenge must be limited to “as applied,” citing In re Directives, 551 F.3d at 1010, which limited the communication service provider’s challenge to “as applied.” Specifically, “[w]here, as here, a statute has been implemented in a defined context, an inquiring court may only consider the statute’s constitutionality in that context; the court may not speculate about the validity of the law as it might be applied in different ways or on different facts.” In turn, In re Directives cited National Endowment for the Arts v. Finley, 524 U.S. 569, 118 S. Ct. 2168 (1998), in which the Court concluded a statute setting some guidelines in awarding financial grants for the arts did not violate the First Amendment. Although the plaintiffs had been denied a grant, the Court held the statute was *facially valid* “as it neither inherently interferes with First Amendment rights nor violates constitutional vagueness principles.” Id. at 573. In doing so, the Court reasoned:

Facial invalidation “is, manifestly, strong medicine” that “has been employed by the Court sparingly and only as a last resort.” Broadrick v. Oklahoma, 413 U.S.

601, 613, 93 S. Ct. 2908, 2916, 37 L. Ed. 2d 830 (1973); see also FW/PBS, Inc. v. Dallas, 493 U.S. 215, 223, 110 S. Ct. 596, 603, 107 L. Ed. 2d 603 (1990) (noting that “facial challenges to legislation are generally disfavored”). To prevail, respondents must demonstrate a substantial risk that application of the provision will lead to the suppression of speech.

Id. at 580.

The Court also noted it was “reluctant, in any event, to invalidate legislation on the basis of its hypothetical application to situations not before the Court.” Id. at 574 (internal quotation omitted).

If I use defendant’s proffered standard in a facial challenge, that there would be a substantial risk the statute would be applied unconstitutionally, rather than the government’s proffered standard, that the statute would survive a facial challenge if there is any set of circumstances in which it could be constitutionally applied,² I would be required to speculate about the other applications. Under the government’s standard, if the statute survives an as-applied challenge, it automatically survives a facial challenge because there is at least one constitutional application. I am unwilling to speculate on other applications with a statute this complex. Moreover, although defendant argues I should undertake a facial challenge to address the lack of procedural safeguards in § 702, the allegedly insufficient procedural safeguards were applied to defendant, so I would address them in an as-applied challenge also. This includes the lack of a warrant, the lack of any probable cause determination, and the lack of any judicial determination about a targeted individual, due to the programmatic nature of § 702 surveillance. This overlap, as well as the complexity, weigh in favor of an as-applied challenge.

² Based on United States v. Salerno, 481 U.S. 739, 745, 107 S. Ct. 2095 (1987).

For these reasons, I will follow the lead of the FISA Court of Review in In re Directives and limit defendant's challenge to an as-applied challenge.

1. Warrant Requirement

Defendant, a U.S. citizen, was not targeted under § 702, but his communications were collected incidentally during intelligence collection targeted at one or more non-U.S. persons outside the United States.

The government contends the warrant requirement is not triggered by the incidental collection of non-targeted U.S. person communications during the lawful collection of communications of targeted non-U.S. persons located outside the United States. According to the government, the privacy interests of the U.S. persons are protected by the required minimization procedures. Application of a warrant requirement in this situation would be impracticable and inconsistent with decades of foreign-intelligence collection practice. The government notes that before starting surveillance of a foreign target, the government cannot know the identities of all people with whom the target will communicate, and there is always a possibility the target will communicate with a U.S. person. Thus, the government claims imposing a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection, even though the foreign targets lack Fourth Amendment rights and their communications often involve only other foreigners. Testimony before Congress supports the government's argument. 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. Comm. on the Judiciary, 110th Cong., 1st Sess. at 8 (Sept. 18, 2007) (statement of

Rep. Forbes) (“would reverse 30 years of established intelligence gathering” and deprive the intelligence community of the flexibility needed to protect the country).

Defendant argues § 702 violates the Fourth Amendment because it permits the “widespread capture, retention, and later querying, dissemination, and use of the communications of American citizens” without the protection afforded by a warrant. Def.’s Mem. in Supp. of Alternative Mot. for Suppression of Evidence 13, ECF No. 503 [hereinafter Def.’s Brief]. Defendant notes the FISC’s statement that the NSA acquires more than 250 million Internet communications each year under § 702, including acquisitions from upstream and from Internet service providers. [Caption Redacted], 2011 WL 10945618, at *9. Defendant speculates that a significant number of those acquisitions would be communications with U.S. persons located in the United States and thus implicate their Fourth Amendment rights sufficiently that the court should apply a warrant requirement.

The government cites cases supporting its argument that applying a warrant requirement to incidental interception of U.S.-person communications during surveillance targeting non-U.S. persons overseas to obtain foreign intelligence is inconsistent with decades of foreign intelligence collection practice. See In re Terrorist Bombings of United States Embassies in East Africa, 552 F.3d 157, 167 (2nd Cir. 2008) (Fourth Amendment’s reasonableness requirement, not the Warrant Clause, governs extraterritorial searches of U.S. citizen’s home and telephone); United States v. Barona, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) (foreign searches historically have not been subject to the warrant procedure).

In addition, “incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.” In re Directives, 551 F.3d at 1015 (in the

context of the PAA). The § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's communications with the extraterritorial target would be lawful. The one distinguishing factor is the possible vast number of incidental communications collected under § 702. I stress the word "possible." It is equally likely that § 702 surveillance of a non-U.S. person located outside the United States would acquire no incidental communications with a U.S. person. Consequently, I am unpersuaded incidental communications collected under § 702 differ sufficiently from previous foreign intelligence gathering to distinguish prior case law, and I hold that § 702 surveillance does not trigger the Warrant Clause.

Alternatively, as I explain in the next section, even if § 702 surveillance triggers the Warrant Clause, no warrant is required because § 702 surveillance falls within the foreign intelligence exception to the warrant requirement.

2. Foreign Intelligence Exception

Assuming the incidental collection of U.S.-person communications under § 702 is subject to the same constitutional scrutiny as foreign intelligence collection targeting U.S. persons, the government contends the Fourth Amendment does not require a warrant for § 702 surveillance because it falls within the foreign intelligence exception.

The Fourth Amendment's warrant requirement applies to domestic national security surveillance. Keith, 407 U.S. at 320. Defendant argues that even if there is a foreign national security exception to the Warrant Clause, the exception's scope is far narrower than the massive surveillance programs under § 702. Defendant claims the reasoning in Keith applies equally well to foreign national security surveillance, especially because of the First Amendment implications in the

seizure of phone calls and emails. Citing several cases, defendant argues “[p]rogrammatic intrusions into privacy generally involve openly implemented safety programs that must be carefully confined to a ‘primary purpose’ other than law enforcement to guard against abuse.” Def.’s Reply 13. See Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 115 S. Ct. 2386 (1995) (program requiring random urinalysis of school athletes to test for drug use, with the purpose of deterring drug use, was constitutional). Because § 702 requires obtaining foreign intelligence to be a *significant* purpose of an acquisition, not a *primary* purpose, defendant argues the bleed-over into criminal investigations is especially high and contends the special needs doctrine should not apply. Defendant is alarmed that the statutory definition of foreign intelligence information in 50 U.S.C. § 1801(e) includes information unrelated to any danger to the country. He also argues that even if the special needs doctrine covers the acquisition of the information, it should not also cover the retention and later querying of the information.

The government disagrees, arguing the special needs exceptions to the Warrant Clause include a foreign intelligence exception. The government cites numerous cases to support its argument and notes that, with the exception of In re Directives, the cases involved the collection of foreign intelligence information from persons *inside* the United States. Because § 702 targets non-U.S. persons reasonably believed to be *outside* the United States, the government contends the analysis in its cases applies even more strongly. The government agrees the amount of intrusiveness and executive discretion are relevant to the reasonableness of a government program designed to serve a special need, but claims those factors do not decide whether the doctrine applies as an exception to the Warrant Clause.

Under this doctrine, the Court has approved exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, makes the warrant and probable-cause requirement impracticable." Griffin v. Wisconsin, 483 U.S. 868, 873, 107 S. Ct. 3164 (1987) (internal quotation omitted). In those situations, the Court "employed a balancing test that weighed 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, 121 S. Ct. 1281 (2001) (special needs doctrine did not apply; Fourth Amendment violated by hospital's performance of urine tests on patients to provide law enforcement evidence of criminal drug use). The Court has approved warrantless searches under the special needs doctrine in various circumstances. See Griffin, 484 U.S. 868 (warrantless searches of probationers' homes to look for contraband); Vernonia, 515 U.S. 646 (school's warrantless drug tests of athletes to deter drug use); Von Raab, 489 U.S. 656 (warrantless drug testing of employees seeking promotion to positions that directly involve the interdiction of illegal drugs or that require the employee to carry a firearm).

Several courts have analyzed and applied the foreign intelligence exception:

After Keith, several courts of appeals, including our own, have examined the Fourth Amendment's application to electronic surveillance conducted under the guise of the President's executive authority to collect foreign intelligence information. These courts 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. See, e.g., United States v. Truong Dinh Hung, 629 F.2d 908, 914 (4th Cir. 1980) ("[B]ecause of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance."); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (holding, in light of the "strong public interest" in uninterrupted foreign intelligence collection, that the Fourth Amendment does not require "prior judicial authorization" of surveillance "conducted and maintained solely for the purpose of gathering foreign

intelligence information”). See generally [United States v. Duggan, 743 F.2d 59, 72 (2d Cir. 1984)] (summarizing foreign intelligence exception cases).

United States v. Duka, 671 F.3d 329, 341 (3rd Cir. 2011) (in analyzing convictions obtained pursuant to a traditional FISA warrant, holding FISA’s amended “significant purpose” requirement is reasonable under the Fourth Amendment).

Notably, the FISA Court of Review applied a foreign intelligence exception “when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.” In re Directives, 551 F.3d at 1012 (requiring a communications service provider to comply with a directive to assist in warrantless surveillance under the PAA). The court reasoned: (1) the purpose of the surveillance went well beyond any “garden-variety” law enforcement objective and involved the acquisition from overseas foreign agents of foreign intelligence to help protect national security; (2) the government’s interest was “particularly intense”; and (3) there was 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.” Id. at 1011-12.

Precisely on point with the case before me, the FISC held that the foreign intelligence exception also applies to § 702 surveillance, even though the court’s understanding of the technical situation underlying the surveillance changed after the government released more information:

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 Docket No. [redacted]. The government’s recent revelations regarding NSA’s acquisition of MCTs [multi-communication transactions] do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection,

NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [redacted] conducted for the purpose of national security—a purpose going “well beyond any garden-variety law enforcement objective.” Further, it remains true that the collection is undertaken in circumstances in which 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.” *Id.* at 36 (quoting *In re Directives* at 18). Accordingly, the government’s revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court’s prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA’s targeting and minimization procedures.

[Caption Redacted], 2011 WL 10945618, at *24 (citation omitted) (granting in part and denying in part the government’s requests for approval of § 702 certifications and procedures; one aspect of the proposed upstream collection of Internet transactions containing MCTs is not reasonable under the Fourth Amendment).

None of defendant’s arguments persuade me to stray from the FISC’s holding. I realize § 702 requires the significant purpose, not the primary purpose, of the acquisition be to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A)(5). The cases discussing the special needs doctrine do not use the phrase “primary purpose” as a term of art, and many do not even use it at all. *See, e.g., Vernonia*, 515 U.S. 646. There is no reasonable argument the government’s need for the acquisitions is merely routine law enforcement. The government’s need for speed and stealth have not lessened since the FISC decided [Caption Redacted], which found that application of the warrant requirement would be impracticable. When I balance the intrusion on the individual’s interest in privacy, namely the incidental collection of U.S. persons’ communications, against these special needs when the government targets a non-U.S. person believed to be outside the United States, I conclude the foreign intelligence exception applies and no warrant is required.

PAGE 31 - OPINION AND ORDER

I will address defendant's concerns about the dual nature of the statutory definition of foreign intelligence information, 50 U.S.C. § 1801(e), in the next section analyzing the reasonableness of the acquisitions.

3. Reasonableness

Application of the foreign intelligence exception does not end the analysis: "even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement." In re Directives, 551 F.3d at 1012.

To analyze whether a government search is reasonable under the Fourth Amendment, the court examines the totality of the circumstances. Samson v. California, 547 U.S. 843, 848, 126 S. Ct. 2193 (2006). The court weighs "'the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy.'" Maryland v. King, 133 S. Ct. 1958, 1970 (2013) (internal quotation omitted) (search using buccal swab inside the cheek to obtain DNA sample after arrest for serious offense is a legitimate police booking procedure that is reasonable under Fourth Amendment).

a. General Contentions

Defendant claims § 702 is presumptively unreasonable because it does not require a warrant, even though the acquired telephone calls and emails are within the core zone of privacy protected from government intrusion. See United States v. Katz, 389 U.S. 347, 353, 88 S. Ct. 507 (1967) (FBI agents' use of an electronic listening device attached to the outside of a phone booth to hear one side of a telephone conversation constituted a search and seizure under the Fourth Amendment); United

States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (warrant requirement applied to emails sent through a commercial internet service provider).

Defendant claims the Warrant Clause is the key metric in determining reasonableness. He disputes that the programmatic authorizations and certifications from the FISC under Title VII offer the protections traditional warrants afford. Defendant lists several protections provided under the Warrant Clause which are missing from § 702 surveillance:

- a) a warrant authorizing the search and seizure; b) based upon probable cause;
- c) particularly describing the place to be searched and the items to be seized; d) based on an affidavit under oath or affirmation; e) issued by a neutral and detached magistrate operating in a judicial capacity; f) with a return or other procedure assuring compliance with the terms of the warrant in its execution.

Def.'s Brief 17-18.

Because § 702 lacks these protections, defendant contends its use is either presumptively unreasonable or, alternatively, the extreme disconnect between § 702 procedures and basic Fourth Amendment warrant protections shows the unreasonableness of searches and seizures under § 702. Even though the FISC approves general programs and procedures under § 702, defendant argues the FISC does not review the government's specific targeting decisions or its later access of seized communications. Defendant contends the government should not be allowed to read the contents of American citizens' electronic communications without a judicial finding of probable cause. Further, defendant argues the government interest in acquiring "foreign intelligence information" is unreasonable under the Fourth Amendment because the term is so broadly defined under 50 U.S.C. § 1801(e), it goes well beyond threats to national security.

According to the government, surveillance under § 702 satisfies the Fourth Amendment's general reasonableness test. It claims the significant interest in national security, in light of FISA's

PAGE 33 - OPINION AND ORDER

statutory safeguards, outweigh the privacy interests of U.S. persons whose communications are incidentally acquired. The government suggests U.S. persons have limited expectations of privacy in electronic communications with non-U.S. persons outside the United States.

The government relies heavily on In re Directives, in which the FISA Court of Review held the PAA, a statute which expired in 2008, was reasonable under the Fourth Amendment. Defendant notes the differences between § 702 and the PAA to argue it is not persuasive when analyzing § 702. First, programs under the PAA did not involve retaining a database of incidentally collected information from non-targeted U.S. persons which could be queried later. In re Directives, 551 F.3d at 1015. Second, because the PAA incorporated § 2.5 of Executive Order 12333, it required an executive determination of probable cause to believe the technique was directed against a foreign power or an agent of a foreign power. Id. at 1014.

I note, importantly, the PAA allowed the government to conduct warrantless foreign intelligence surveillance on targets reasonably believed to be located outside the United States, *including* U.S. persons. In re Directives, 551 F.3d at 1006. Section 702 prohibits targeting U.S. persons, even if they are outside the United States. 50 U.S.C. § 1881a(b)(3). In this respect, the PAA allowed much broader surveillance than § 702 does. I consider this difference significant and believe the analysis in In re Directives is particularly instructive.

b. Comparison of Section 702 to Protections Afforded by a Warrant

I will first address defendant's arguments comparing the protections provided by a warrant to those provided under § 702.

The Fourth Amendment states, in part: “no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

In specifically addressing arguments about prior judicial review, probable cause, and particularity, the FISA Court of Review refused to “reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable.” In re Directives, 551 F.3d at 1013. The court explained, “the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds.” Id. With this guidance in mind, I turn to the arguments.

Without the protections of the particularity requirement, defendant contends the communications of American citizens are swept up by § 702 surveillance in a dragnet fashion prohibited by the Fourth Amendment. Defendant also contrasts the Warrant Clause’s requirement of a supporting affidavit under oath with the § 702 procedures for authorization. Defendant is concerned the § 702 procedures fall far short of the oath or affirmation provision of the Warrant Clause, particularly because the certification does not deal with particular persons or events.

The government notes the Attorney General and DNI must certify that targeting and minimization procedures are in place which are consistent with the Fourth Amendment and that a significant purpose of the acquisition is to obtain foreign intelligence information. The government contends the certification requirement represents an important internal check on the actions of the Executive Branch. It claims defendant’s argument, that the government may target entire geographical areas or groups of people or read every American communication with a country of interest, is an accusation the government will not abide by the required procedures, despite extensive

oversight. To the contrary, the government argues the targeting procedures determine that “the 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.

The lack of an oath requirement in § 702, as well as any argument the government will not follow the law, is unpersuasive. Absent evidence of fraud or misconduct, a presumption of regularity attaches to obtaining a warrant. The FISA Court of Review applied the same presumption to the government’s procurement of a directive to a communications service provider under the PAA. In re Directives, 551 F.3d at 1014-15. I have seen no evidence of government fraud or misconduct in this case, and the differences between the PAA and § 702 do not weigh against applying the same presumption of regularity here.

Turning to the particularity requirement, § 702 surveillance uses targeting and minimization procedures approved by the FISC. [Caption Redacted], 2011 WL 10945618, at *6 (“The Court found in those prior dockets that the targeting and minimization procedures [as applied to forms of to/from communications that have previously been described to the Court] were consistent with the requirements of 50 U.S.C. § 1881a(d)(e) and with the Fourth Amendment.”).³ Section 702 limits surveillance only to non-U.S. persons reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(b). A significant purpose of the acquisition must be to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A)(5).

³ Although [Caption Redacted] ultimately found the targeting and minimization procedures related to multi-communication transactions unreasonable under the Fourth Amendment, 2011 WL 10945618, at *28, the unconstitutional procedures were submitted to the FISC in April 2011, well after defendant was arrested.

The FISA Court of Review concluded the PAA's pre-surveillance procedures were sufficient to satisfy Fourth Amendment concerns. In re Directives, 551 F.3d at 1013. I am aware the PAA's incorporation of Executive Order 12333 included a requirement that surveillance targeting U.S. persons reasonably believed to be outside the United States had to be based on a finding by the Attorney General of probable cause to believe the target was a foreign power or agent of a foreign power. Section 702 has no such probable cause requirement. Section 702, however, prohibits targeting a U.S. person under any circumstances, even if the person is located outside the United States and acting as a foreign power or agent of a foreign power. Consequently, I conclude this difference does not diminish the particularity to the point of making the collections unreasonable under the Fourth Amendment.

The warrant and an inventory of seized property are returned to the issuing judge under Rule 41, and there are provisions to convey this information to the person whose property was seized. Defendant observes there are no similar provisions for a § 702 seizure. He argues the lack of notice and accountability under § 702 mean the person is never notified of the seizure, the searchers get no guidance on the limits of what can be read, and there is no process by which the FISC can know if the search and seizure were within the scope of the authorization.

The same notice provisions under 50 U.S.C. § 1806(c) cover FISA Title I/III, under which courts have long held surveillance is constitutional, and § 702. Importantly, defendant has now had full notice, giving him the ability to challenge the search and seizure. Minimization procedures, discussed in more detail below, provide guidance about what can be read. The FAA has oversight provisions requiring the Attorney General and DNI to regularly report compliance with targeting and

minimization procedures, as well as other data, to the FISC and congressional intelligence and judiciary committees. 50 U.S.C. § 1881a(l).

In sum, I do not find the lack of procedures associated with warrants make § 702 searches unreasonable under the Fourth Amendment.

c. Balancing the Governmental Interests Against the Intrusion on Privacy

I will now turn to balancing the legitimate governmental interests against the intrusion on an individual's privacy.

It is undisputed the government's interest in protecting the national security is compelling. "It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." Haig v. Agee, 453 U.S. 280, 307, 101 S. Ct. 2766 (1981) (internal quotation omitted) (the President has authority to revoke a passport because the person's activities in foreign countries are causing or are likely to cause serious damage to the national security or foreign policy of the United States). "[T]he Government's interest in combating terrorism is an urgent objective of the highest order." Holder v. Humanitarian Law Project, 561 U.S. 1, 28, 130 S. Ct. 2705 (2010) (analyzing statute criminalizing providing material support to foreign terrorist organization).

Defendant points to the statutory definition of foreign intelligence information to argue the government interest is too broadly defined, and thus intrudes on individual privacy too much, to justify the mass acquisition of Americans' electronic communications. The statute states:

(e) "Foreign intelligence information" means—

(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).

The FISA Court of Review describes subsection (2) as “information referred to as ‘affirmative’ or ‘positive’ foreign intelligence information rather than . . . ‘protective’ or ‘counterintelligence’ information. In re Sealed Case, 310 F.3d at 723, n.9. Defendant is concerned the government could interpret the “conduct of the foreign affairs of the United States” broadly enough to cover such items as international trade, rather than just threats to national security.

I note the discovery in this case all concerned protecting the country from a terrorist threat and did not stray into the broader category of the conduct of foreign affairs. I discuss this further in the classified opinion.

Under § 702, the intrusion of an individual’s privacy is due to the incidental collection of the individual’s communications during the acquisition of the communications from a targeted non-U.S. person reasonably believed to be outside the United States.⁴ The government contends U.S. persons have limited expectations of privacy when communicating electronically with non-U.S. persons outside the United States. The government reasons the U.S. person assumes the risk that the foreign

⁴ Defendant does not argue he was mistakenly targeted.

recipient will give the information to others, leave it freely accessible to others, or that the U.S. or foreign government will obtain the information.

The Fourth Amendment does not prohibit the government from obtaining information a person revealed to a third party, even if revealed in confidence. United States v. Miller, 425 U.S. 435, 444, 96 S. Ct. 1619 (1976) (bank records). This concept also applies to electronic communications. “A person’s reasonable expectation of privacy may be diminished in transmissions over the Internet or e-mail that have already arrived at the recipient.” United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (internal quotation omitted).

Defendant offers the government cannot seize these communications without the consent of the recipient, which is an argument in favor of only the recipient’s expectation of privacy in the communication. The sender’s expectation of privacy has still been diminished.

Defendant also claims the minimization procedures for § 702 surveillance, as defined in 50 U.S.C. § 1801(h), provide no meaningful protection because the exclusions from the minimization procedures swallow the rule. As a result, the illusory minimization procedures make § 702 search and seizures unreasonable under the Fourth Amendment.

As I explain next, I conclude the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment.

The government refers to a recently declassified document to support the reasonableness of § 702 minimization procedures.⁵ The government also notes the FISC has repeatedly found

⁵ Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (dated October 31, 2011), available at <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>.

materially equivalent minimization procedures sufficient in the context of traditional FISA electronic surveillance and physical search. Because these searches target U.S. persons in the United States, they are more likely to capture communications of non-targeted U.S. persons than the foreign communications captured under § 702. The government additionally relies on the FAA's oversight provisions requiring regular reports to the FISC and congressional oversight committees on the implementation of minimization procedures and the FISC's Rule of Procedure 13(b) which requires the government to report all instances of non-compliance.

The FISC has concluded the § 702 minimization procedures are consistent with the Fourth Amendment. [Caption Redacted], 2011 WL 10945618, at *6. In finding the PAA constitutional, the FISA Court of Review commented:

It is also significant that effective minimization procedures are in place. These procedures 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. The minimization procedures implemented here are almost identical to those used under FISA [Title I/III] to ensure the curtailment of both mistaken and incidental acquisitions.

In re Directives, 551 F.3d at 1015.

Section 6 of the declassified minimization procedures discusses the retention and dissemination of foreign communications of or concerning United States persons, putting limits on both. For example, the identity of the United States person is deleted in any dissemination of the information unless certain requirements are met. I do not agree with defendant that the minimization procedures provide no meaningful protection. On the contrary, I agree with the FISC that the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment.

d. Querying After Acquisition

I now turn to defendant's most persuasive argument. He argues that even if § 702 warrantless surveillance is lawful, subsequent querying of the information after acquisition is a search requiring a warrant under the Fourth Amendment. Defendant draws analogies to United States v. Sedaghaty, 728 F.3d 885, 910-13 (9th Cir. 2013) (in a computer search authorized by warrant, the court rejected expansion of the warrant's expressly limited scope of items to be seized to include evidence related to background information providing a motive for the alleged crimes and stated in the affidavit supporting the warrant), United States v. Mulder, 808 F.2d 1346, 1348 (9th Cir. 1987) (pills lawfully in government possession could have been field tested for illegal drugs under a limited warrant exception, but laboratory testing to determine precise molecular structure required a warrant), and United States v. Young, 573 F.3d 711, 720-21 (9th Cir. 2009) (warrant required to search contents of a backpack taken by hotel security without evicting guest, and then given to police).

The government strongly disagrees. It distinguishes defendant's cases as analyzing government action beyond the scope of the warrant (or warrant exception). I agree with this characterization. Sedaghaty analyzed seizing evidence quite dissimilar from the items the warrant stated in its expressly limited list; Mulder and Young discussed whether to expand the private search warrant exception, as explained in United States v. Jacobsen, 466 U.S. 109, 104 S. Ct. 1652 (1984). As a result, I cannot draw analogies from these cases to support defendant's arguments.

Unfortunately, I do not find much assistance in most of the government's analogies either. Law enforcement computer queries of license plates and driver's licenses take place in a highly regulated arena and, in the case of license plates, are based on information displayed for all to see.

United States v. Diaz-Castaneda, 494 F.3d 1146, 1151-53 (9th Cir. 2007) (no reasonable expectation of privacy in a license plate so querying government databases about it is not a Fourth Amendment search; police can ask for identification of people who are legitimately stopped without performing a Fourth Amendment search). DNA profiles retained in a database to allow later law enforcement searches are from people who have been arrested or convicted. Boroian v. Mueller, 616 F.3d 60, 67-68 (1st Cir. 2010) (“government’s retention and matching of [former probationer’s] profile against [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”). Neither of these limited invasions of privacy can be compared to the incidental acquisition of communications of U.S. persons.

The government also draws an analogy to minimization procedures under the Federal Wiretap Act which allow the government to use evidence from a wiretap to prove a crime unrelated to the original purpose for the wiretap. This analogy is more helpful because it addresses the use of communications obtained incidentally to those acquired by the wiretap. Specifically:

When an authorized wiretap intercepts communications relating to offenses other than those specified in the order of authorization, 18 U.S.C. § 2517(5), disclosure or use of those communications is permissible provided a subsequent application . . . made to a judge of competent jurisdiction [demonstrates] the good faith of the original application. Such subsequent application would include a showing that the original order was lawfully obtained, that it was sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order.

United States v. Goffer, 721 F.3d 113, 122-23 (2nd Cir. 2013) (internal quotations and citations omitted), pet. for cert. filed, No. 13-9973 13A777 (Apr. 2, 2014).

Because the government complied with all § 702 procedures concerning targeting and minimization, the government contends its actions were within the scope of the relevant legal authority and are thus distinguishable from defendant's cases. In its view, subsequent queries of information lawfully obtained, which do not implicate any reasonable expectation of privacy beyond that implicated in the initial lawful collection, do not constitute separate searches under the Fourth Amendment. The government claims this is true even if U.S. person identifiers are used in the querying.

The government notes the minimization procedures compel it to review information lawfully collected under § 702, which includes information about U.S. persons, to determine if the information should be retained or disseminated. According to the government:

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. Querying lawfully collected information using U.S.-person identifiers does not involve a significant additional intrusion on a person's privacy, beyond the level of intrusion already occasioned by the government as it reviews and uses information it lawfully collects under Section 702 pursuant to its need to analyze whether the information should be retained or disseminated.

Govt.'s Brief 57-58.

In the government's view, it must conduct such queries to fulfill its compelling interest to detect and disrupt terrorist attacks by discovering potential links between foreign terrorist groups and people within the United States.

It is true, the FISC has approved minimization procedures which allow querying using U.S. person identifiers. [Caption Redacted], 2011 WL 10945618, at *8. While the procedures previously imposed a "wholesale bar" on such queries, the new approved procedures allowed queries with U.S. person identifiers "subject to approval pursuant to internal NSA procedures and oversight by the

Department of Justice.” Id. The FISC reasoned it had approved FISA Title I applications targeting U.S. persons that used minimization procedures allowing queries with U.S. person identifiers.

It follows that the substantially-similar querying provision found at Section 3(b)(5) of 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.

This is a very close question. On the one hand, why not require a warrant when using a U.S. person identifier to search a database of information already gathered? That is not the test, however—just because a practice might better protect Americans’ privacy rights does not mean the Fourth Amendment requires the practice. Indeed, as the government argues, it must review information lawfully collected to decide whether to retain or disseminate it under the minimization procedures. As the FISC reasoned, the § 702 collection, by being aimed at non-U.S. persons believed to be outside the United States, is less likely to acquire information about non-consenting U.S. persons than a FISA Title I collection. I do not find any significant additional intrusion past what must be done to apply minimization procedures. Thus, subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment.

e. Summary

To sum up, I must examine the totality of the circumstances and weigh the government’s compelling interest in protecting national security against the degree to which § 702 surveillance intrudes on an individual’s privacy. See Samson, 547 U.S. at 848; King, 133 S. Ct. at 1970.

Section 702 has numerous safeguards built into the statute. Most importantly, § 702 is aimed at acquiring foreign intelligence information in electronic communications from non-U.S. persons located outside the United States. There are additional limitations, including that the statute cannot “intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States[.]” 50 U.S.C. § 1881a(b)(2). Minimization procedures protect the privacy of U.S. persons whose communications are incidentally acquired. The Attorney General and DNI must certify, among other things, that appropriate targeting and minimization procedures are in place and a significant purpose of the acquisition is to obtain foreign intelligence information. 50 U.S.C. § 1881a(g)(2)(A). The FISC must find the targeting and minimization procedures consistent with the Fourth Amendment. Congress and the FISC provide oversight based on specific reporting requirements.

Based on the statutory protections, I conclude the government’s compelling interest in protecting national security outweighs the intrusion of § 702 surveillance on an individual’s privacy. Accordingly, § 702, as applied to defendant, is reasonable under the Fourth Amendment.

E. Acquisition of Section 702 Materials in this Case

Even if the court concludes § 702 is constitutional, defendant correctly notes that any acquisition, retention, accessing, dissemination, and use of the seized electronic communications which exceed the FISC authorizations are unlawful. Defendant’s concerns are heightened by declassified FISC opinions indicating that some § 702 surveillance might have exceeded the authorizations. Defendant asks the court to obtain extensive background material to assure the

surveillance was lawfully conducted under the statute and, if not, to suppress all evidence derived from it.

The government contends once I perform an in camera, ex parte review of the relevant classified materials, I will conclude the § 702 acquisition was lawfully authorized and conducted.

I made a careful de novo, ex parte review of the § 702 applications and conclude the certification required by 50 U.S.C. § 1881a(g)(2)(A) was in place. I also find that the government agents followed appropriate targeting and minimization procedures. Thus, I conclude the § 702 surveillance at issue here was lawfully conducted.

F. Suppression Based on Other Alleged Surveillance Activities

Defendant raises concerns about the collection of telephone metadata under § 215 of the Patriot Act, codified at 50 U.S.C. § 1861, and any other still-secret warrantless surveillance programs. He assumes there is a strong possibility that his telephone metadata has been collected, and he asks the court to address the lawfulness of these programs, conclude they violate the First and Fourth Amendments, and suppress all fruits of these other surveillance activities.

I deny defendant's arguments concerning § 215 for the reasons stated in the classified opinion.

G. Good Faith Exception

As an alternative argument, the government claims the good faith exception to the exclusionary rule, as set forth in United States v. Leon, 468 U.S. 897 (1984), provides an independent basis for denying defendant's suppression motion. The government argues the exception applies here because the § 702 collection was authorized by a duly-enacted statute, law

enforcement officers reasonably relied on orders of a neutral magistrate, namely the judges of the FISC, and the FISA Court of Review has upheld similar directives issued under the PAA.

Defendant contends the court should not attach a good faith exception to FISA because the statute, which preceded Leon, does not contain an exception in its statutory suppression provision, 50 U.S.C. § 1806(g). Defendant distinguishes the government's other cases because they address situations where officers relied on an individualized FISA or other judicial order, which was not done here. See United States v. Ning Wen, 477 F.3d 896, 897-98 (7th Cir. 2007) (FISA warrant). Defendant further claims the government knew of the constitutional objections from the day of enactment of the FAA due to the immediate initiation of litigation in Clapper.

I will first address defendant's last argument concerning the initiation of litigation against § 702. I see no reason for the government to assume all challenges to a statute will be successful; numerous warrants issued under FISA Title I/III have survived challenges. A statute is constitutional until a court declares otherwise. Moreover, even the defendant who succeeds in having a statute declared unconstitutional is not guaranteed application of the exclusionary rule. See Duka, 671 F.3d at 346 (quoted below).

Under the good faith exception to the exclusionary rule established in Leon, the government has the burden of demonstrating the officer acted "'in objectively reasonable reliance' on the warrant." United States v. Underwood, 725 F.3d 1076, 1085 (9th Cir. 2013) (quoting Leon, 468 U.S. at 922)).⁶ "Exclusion is not a personal constitutional right, nor is it designed to redress the

⁶ There are four situations that per se fail to satisfy the good faith exception, as explained in Underwood, but they do not fit well into the issue before me because the situations assume the exception is being applied to a warrant.

In these situations, "the officer will have no reasonable grounds for believing that

injury occasioned by an unconstitutional search.” Davis v. United States, 131 S. Ct. 2419, 2426 (2011) (internal quotations omitted) (refusing to apply exclusionary rule when police conduct a search in objectively reasonable reliance on binding appellate precedent). Even if a court finds the statute on which a warrant is based unconstitutional, the evidence is not automatically suppressed:

The Supreme Court has ruled categorically that “suppress[ing] evidence obtained by an officer acting in objectively reasonable reliance on a statute” would not further the purposes of the exclusionary rule, even if that statute is later declared unconstitutional. Illinois v. Krull, 480 U.S. 340, 349–50, 107 S. Ct. 1160, 94 L. Ed. 2d 364 (1987). Therefore, even a defendant who can establish that evidence against him or her was procured under a statute that violates the Fourth Amendment is not entitled to have such evidence excluded from his or her criminal trial unless he or she can establish that the officer’s reliance on the statute was not objectively reasonable.

Duka, 671 F.3d at 346 (after finding FISA’s amended “significant purpose” test was reasonable under the Fourth Amendment, the Third Circuit alternatively held it would not apply the exclusionary rule to evidence obtained under a FISA *warrant*, even if it had held FISA was unconstitutional).

Defendant’s argument, based on the fact that there is no exception in FISA’s statutory exclusion provision, draws an analogy to wiretaps under Title III. Some courts have held the good faith exception to the warrant requirement does not apply to wiretap warrants under Title III. United States v. Rice, 478 F.3d 704, 711 (6th Cir. 2007) (“the language in Title III provides that exclusion is

the warrant was properly issued.” 468 U.S. at 922–23, 104 S. Ct. 3405. The four situations are: (1) where the affiant recklessly or knowingly placed false information in the affidavit that misled the issuing judge; (2) where the judge “wholly abandon[s] his [or her] judicial role”; (3) where the affidavit is “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable”; and (4) where the warrant is “so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.” Id.

Underwood, 725 F.3d at 1085.

PAGE 49 - OPINION AND ORDER

the exclusive remedy for an illegally obtained warrant. In contrast to the law governing probable cause under the Fourth Amendment, the law governing electronic surveillance via wiretap is codified in a comprehensive statutory scheme providing explicit requirements, procedures, and protections.”). Other courts have held the opposite. United States v. Moore, 41 F.3d 370, 376 (8th Cir. 1994) (good faith exception can apply to warrants under Title III); United States v. Malekzadeh, 855 F.2d 1492, 1497 (11th Cir.1988) (same). The Ninth Circuit has not expressly analyzed application of the good faith exception to evidence obtained pursuant to a Title III wiretap. See United States v. Duran, 189 F.3d 1071, 1084-87 (9th Cir. 1999) (court did not exclude wiretap evidence after concluding Title III preconditions to judicial authorization of wiretap were satisfied even though the application did not cover the possibility the target might purchase a new cell phone; court did not address government’s proffered good faith exception). Defendant asks me to apply the Sixth Circuit holding to § 702.

With the split in the circuits and no Ninth Circuit precedent, little is to be gained from analogizing § 702 to Title III wiretaps. I will proceed instead to the policy reasons behind the exclusionary rule. I also must examine the policy reasons because there is no traditional warrant under § 702. That was the case in Krull, in which the Court expanded the Leon good faith exception and did not exclude evidence obtained by police acting in objectively reasonable reliance on a state vehicle code authorizing warrantless administrative searches, even though a court later held the statute violated the Fourth Amendment. Krull, 480 U.S. at 349-50, 356-57. The Court reasoned the prime purpose of the exclusionary rule was to “deter future unlawful police conduct”; it was not meant to punish judges or magistrates. Id. at 347, 348. In extending the good faith exception, the Court likened the role of a magistrate in issuing warrants to the role of a legislature in passing legislation:

PAGE 50 - OPINION AND ORDER

The approach used in Leon is equally applicable to the present case. The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant. Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law. If the statute is subsequently declared unconstitutional, excluding evidence obtained pursuant to it prior to such a judicial declaration will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to enforce the statute as written.

Id. at 349.

Addressing an argument that applies equally well to § 702 surveillance, the Court was also unpersuaded by the fact that a “statute authorizing warrantless administrative searches affects an entire industry and a large number of citizens, while the issuance of a defective warrant affects only one person.” Id. at 350.

Real deterrent value is a “necessary condition for exclusion,” but it is not “a sufficient” one. Hudson v. Michigan, 547 U.S. 586, 596, 126 S. Ct. 2159, 165 L. Ed. 2d 56 (2006). The analysis must also account for the “substantial social costs” generated by the rule. Leon, supra, at 907, 104 S. Ct. 3405. Exclusion exacts a heavy toll on both the judicial system and society at large. Stone, 428 U.S., at 490–491, 96 S. Ct. 3037. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. Ibid. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. See Herring, supra, at 141, 129 S. Ct. 695. Our cases hold that society must swallow this bitter pill when necessary, but only as a “last resort.” Hudson, supra, at 591, 126 S. Ct. 2159. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs. See Herring, supra, at 141, 129 S. Ct. 695; Leon, supra, at 910, 104 S. Ct. 3405.

Davis, 131 S. Ct. at 2427.

Here, the § 702 surveillance was based on a statute Congress enacted and a certification the FISC approved. Law enforcement was only acting based on the FISC's approval. The judicial approval makes law enforcement's reliance more objectively reasonable than the officer's reliance in

Krull, in which the administrative search took place under a statute that required no judicial approval of the programs based on it. Even if I found § 702 unconstitutional, exclusion of the evidence here would not deter unconstitutional actions by law enforcement. For these reasons, I conclude the good faith exception should apply.

H. Request for Franks Hearing

Defendant seeks a hearing under Franks v. Delaware, 438 U.S. 154 (1978), to challenge the validity of the representations made to the FISC to obtain the FISA warrants already considered by the court in this case.

In Franks, the Supreme Court held that, under certain circumstances, a defendant is entitled to an evidentiary hearing in which he can attack the veracity of a search warrant affidavit or challenge the omission of material facts in the affidavit. When a defendant seeks a Franks hearing because of “allegations of material false statements or omissions in an affidavit supporting a search warrant, a defendant must make a substantial preliminary showing that false or misleading statements were (1) deliberately or recklessly included in an affidavit submitted in support of a search warrant; and (2) necessary to the finding of probable cause.” United States v. Flyer, 633 F.3d 911, 916 (9th Cir. 2011) (internal quotations omitted).

Defendant argues the existence of previously undisclosed surveillance under § 702 and telephone metadata collection programs raise serious questions on whether the government reported the entire story to the FISC in the applications. Defendant argues he is precluded from making the normal substantial preliminary showing to obtain a Franks hearing because the government and the court have refused to disclose the FISA warrant applications.

The government responds that defendant's lack of access to the FISA applications does not ease his burden to make a substantial preliminary showing of misrepresentations essential to the finding of probable cause or, in the case of § 702 surveillance, essential to support the certification from the Attorney General and DNI. Moreover, the government insists defendant's allegations about the government's lack of candor to the court in other federal cases involving national security issues cannot establish that any errors were made in this case.

I must agree with the government on the last point. If misrepresentations in one case were attributed to the government in unrelated cases, all defendants would be entitled to a Franks hearing without making the required preliminary showing.

Defendant's position has not changed since the pretrial FISA suppression motion—he can only speculate about false statements or omissions. This is insufficient to qualify as a substantial preliminary showing. I realize the difficult position the defense team is in, but the denial of a Franks hearing is commonplace in the FISA context and goes hand-in-hand with the ex parte judicial review process. See United States v. Abu-Jihaad, 630 F.3d 102, 130 (2nd Cir. 2010); United States v. el-Mezain, 664 F.3d 467, 570 (5th Cir. 2011); United States v. Damrah, 412 F.3d 618, 624-25 (6th Cir. 2005). Cf. United States v. Daoud, No. 14-1284, 2014 WL 2696734 (7th Cir. June 16, 2014) (Rovner, J., concurring) (explaining difficulties defendants face in getting a Franks hearing in the FISA context).

I. Renewed Motion for Discovery

Although FISA allows the court to make an in camera, ex parte review of materials when deciding a motion to suppress, the statute does allow the aggrieved person to receive discovery in certain circumstances. Specifically, “In making this determination, 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).

Defendant renews his motion for discovery so he may hone his arguments. He insists the court should interpret the term “necessary” in § 1806(f) to mean something closer to “helpful” or “appropriate” and not “absolutely necessary” or “essential.”

I am aware of a single district court which granted defendant’s motion for disclosure of FISA materials to defense counsel with security clearances. United States v. Daoud, No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014) (order stayed pending appeal). The government’s only response to the motion was that disclosure had never been ordered. The court found the response inadequate to explain how national security would be harmed by disclosure to properly cleared defense counsel. Id. at *2. The Seventh Circuit just reversed the district court, however, holding the court cannot order disclosure of the classified materials without first finding that the “disclosure is necessary to make an accurate determination of the legality of the surveillance[,]” as provided in FISA. United States v. Daoud, 2014 WL 2696734. The Circuit further held that it was possible for the court to determine the legality of the investigation without disclosure of the classified materials to defense counsel, and that the investigation did not violate FISA. Id.

I am unconvinced by both defendant’s arguments and the district court in Daoud—classified material is at issue here. The Ninth Circuit has rejected the argument that FISA materials can be turned over if defense counsel has the appropriate security clearances:

PAGE 54 - OPINION AND ORDER

Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy security clearance. We reject the notion that a defendant's due process right to disclosure of FISA materials turns on the qualifications of his counsel.

United States v. Ott, 827 F.2d 473, 477 (9th Cir. 1987) (holding FISA's *ex parte in camera* proceedings do not violate due process, even though defense counsel had high security clearances).

"[D]isclosure of FISA materials is the exception and *ex parte, in camera* determination is the rule." Abu-Jihaad, 630 F.3d at 129 (internal quotation omitted); el-Mezain, 664 F.3d at 567 (same, quoting Abu-Jihaad). Obviously it would be helpful to the court to have defense counsel review the materials prior to making arguments. Congress, however, did not put "helpful" in the statute; it chose "necessary." I interpret "necessary" to be much closer to "essential" than to "helpful." And I do not find disclosure to the defense is necessary for me to make an accurate determination of the legality of the surveillance.

Moreover, in my review of the FISA materials associated with this motion and the previous FISA suppression motion, I have seen "no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure" here. Ott, 827 F.2d at 476 (internal quotation omitted).

Accordingly, I deny defendant's motion for discovery.

CONCLUSION

Defendant's Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the

Pretrial Notice Statute [500], defendant's Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance [502], and defendant's Second Motion for a New Trial [504] are denied.

IT IS SO ORDERED.

Dated this 24th day of June, 2014.

/s/ Garr M. King
Garr M. King
United States District Judge

“(5) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

50 USC 1881a. **“SEC. 702. PROCEDURES FOR TARGETING CERTAIN PERSONS OUTSIDE THE UNITED STATES OTHER THAN UNITED STATES PERSONS.**

“(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

“(b) LIMITATIONS.—An acquisition authorized under subsection (a)—

“(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

“(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

“(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

“(4) 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; and

“(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

“(c) CONDUCT OF ACQUISITION.—

“(1) IN GENERAL.—An acquisition authorized under subsection (a) shall be conducted only in accordance with—

“(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

Certification.

“(B) upon submission of a certification in accordance with subsection (g), such certification.

“(2) DETERMINATION.—A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the implementation of such authorization.

“(3) TIMING OF DETERMINATION.—The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)—

“(A) before the submission of a certification in accordance with subsection (g); or

“(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

“(4) CONSTRUCTION.—Nothing in title I shall be construed to require an application for a court order under such title

for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

"(d) TARGETING PROCEDURES.—

"(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to—

"(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

"(B) 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.

"(2) JUDICIAL REVIEW.—The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

"(e) MINIMIZATION PROCEDURES.—

"(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate, for acquisitions authorized under subsection (a).

"(2) JUDICIAL REVIEW.—The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

"(f) GUIDELINES FOR COMPLIANCE WITH LIMITATIONS.—

"(1) REQUIREMENT TO ADOPT.—The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure—

"(A) compliance with the limitations in subsection (b); and

"(B) that an application for a court order is filed as required by this Act.

"(2) SUBMISSION OF GUIDELINES.—The Attorney General shall provide the guidelines adopted in accordance with paragraph (1) to—

"(A) the congressional intelligence committees;

"(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

"(C) the Foreign Intelligence Surveillance Court.

"(g) CERTIFICATION.—

"(1) IN GENERAL.—

"(A) REQUIREMENT.—Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

"(B) EXCEPTION.—If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for **Deadline.**

such authorization as soon as practicable but in no event later than 7 days after such determination is made.

“(2) REQUIREMENTS.—A certification made under this subsection shall—

“(A) attest that—

“(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

“(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

“(II) 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;

“(ii) the minimization procedures to be used with respect to such acquisition—

“(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

“(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

“(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;

“(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

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

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

“(vii) the acquisition complies with the limitations in subsection (b);

“(B) include the procedures adopted in accordance with subsections (d) and (e);

“(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

“(i) appointed by the President, by and with the advice and consent of the Senate; or

“(ii) the head of an element of the intelligence community;

“(D) include—

“(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

Effective date.

“(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

“(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

“(3) CHANGE IN EFFECTIVE DATE.—The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

“(4) LIMITATION.—A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

“(5) MAINTENANCE OF CERTIFICATION.—The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

“(6) REVIEW.—A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

“(h) DIRECTIVES AND JUDICIAL REVIEW OF DIRECTIVES.—

“(1) AUTHORITY.—With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—

“(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

“(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

“(2) COMPENSATION.—The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

“(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

“(4) CHALLENGING OF DIRECTIVES.—

“(A) AUTHORITY TO CHALLENGE.—An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set

aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

Deadline. “(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) not later than 24 hours after the filing of such petition.

“(C) STANDARDS FOR REVIEW.—A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

Deadline. “(D) PROCEDURES FOR INITIAL REVIEW.—A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it.

Records. Upon making a determination under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

Deadline. “(E) PROCEDURES FOR PLENARY REVIEW.—If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

Records.

“(F) CONTINUED EFFECT.—Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

“(G) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

“(5) ENFORCEMENT OF DIRECTIVES.—

“(A) ORDER TO COMPEL.—If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

Deadline. “(B) ASSIGNMENT.—The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section

103(e)(1) not later than 24 hours after the filing of such petition.

“(C) PROCEDURES FOR REVIEW.—A judge considering a petition filed **Deadline.** under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons **Records.** for a determination under this paragraph.

“(D) CONTEMPT OF COURT.—Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

“(E) PROCESS.—Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

“(6) APPEAL.—

“(A) APPEAL TO THE COURT OF REVIEW.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The **Records.** Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

“(B) CERTIORARI TO THE SUPREME COURT.—The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

“(i) JUDICIAL REVIEW OF CERTIFICATIONS AND PROCEDURES.—

Deadlines.

“(1) IN GENERAL.—

“(A) REVIEW BY THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

“(B) TIME PERIOD FOR REVIEW.—The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

“(C) AMENDMENTS.—The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including

if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

“(2) REVIEW.—The Court shall review the following:

“(A) CERTIFICATION.—A certification submitted in accordance with subsection (g) to determine whether the certification contains all the required elements.

“(B) TARGETING PROCEDURES.—The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to—

“(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

“(ii) 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.

“(C) MINIMIZATION PROCEDURES.—The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) or section 301(4), as appropriate.

“(3) ORDERS.—

“(A) APPROVAL.—If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

“(B) CORRECTION OF DEFICIENCIES.—If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order—

“(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

Deadline.

"(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

"(C) REQUIREMENT FOR WRITTEN STATEMENT.—In support of an **Records.** order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

"(4) APPEAL.—

"(A) APPEAL TO THE COURT OF REVIEW.—The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, **Records.** reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

"(B) CONTINUATION OF ACQUISITION PENDING REHEARING OR APPEAL.—Any acquisition affected by an order under paragraph (3)(B) may continue—

"(i) during the pendency of any rehearing of the order by the Court en banc; and

"(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

"(C) IMPLEMENTATION PENDING APPEAL.—Not later than 60 days **Deadline.** after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

"(D) CERTIORARI TO THE SUPREME COURT.—The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be **Records.** transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

"(5) SCHEDULE.—

"(A) REAUTHORIZATION OF AUTHORIZATIONS IN EFFECT.—If the **Deadline.** Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

"(B) REAUTHORIZATION OF ORDERS, AUTHORIZATIONS, AND DIRECTIVES.—If the Attorney General and the Director of National Intelligence **Applicability.** seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues

an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

“(j) JUDICIAL PROCEEDINGS.—

“(1) EXPEDITED JUDICIAL PROCEEDINGS.—Judicial proceedings under this section shall be conducted as expeditiously as possible.

Applicability.

“(2) TIME LIMITS.—A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

“(k) MAINTENANCE AND SECURITY OF RECORDS AND PROCEEDINGS.—

“(1) STANDARDS.—The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

“(2) FILING AND REVIEW.—All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

“(3) RETENTION OF RECORDS.—The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period of not less than 10 years from the date on which such directive or such order is issued.

“(l) ASSESSMENTS AND REVIEWS.—

Deadlines.

“(1) SEMIANNUAL ASSESSMENT.—Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to—

“(A) the Foreign Intelligence Surveillance Court; and

“(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

“(i) the congressional intelligence committees; and

“(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

“(2) AGENCY ASSESSMENT.—The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General—

“(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

“(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-

person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

“(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

“(D) shall provide each such review to—

“(i) the Attorney General;

“(ii) the Director of National Intelligence; and

“(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

“(I) the congressional intelligence committees; and

“(II) the Committees on the Judiciary of the House of Representatives and the Senate.

“(3) ANNUAL REVIEW.—

“(A) REQUIREMENT TO CONDUCT.—The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)—

“(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

“(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

“(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

“(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

“(B) USE OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

“(C) PROVISION OF REVIEW.—The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to—

“(i) the Foreign Intelligence Surveillance Court;

“(ii) the Attorney General;

“(iii) the Director of National Intelligence; and

“(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution—

“(I) the congressional intelligence committees; and

“(II) the Committees on the Judiciary of the House of Representatives and the Senate.

50 USC 1881b. “SEC. 703. CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES.

“(a) JURISDICTION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—

“(1) IN GENERAL.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

“(2) LIMITATION.—If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect. Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.

“(b) APPLICATION.—

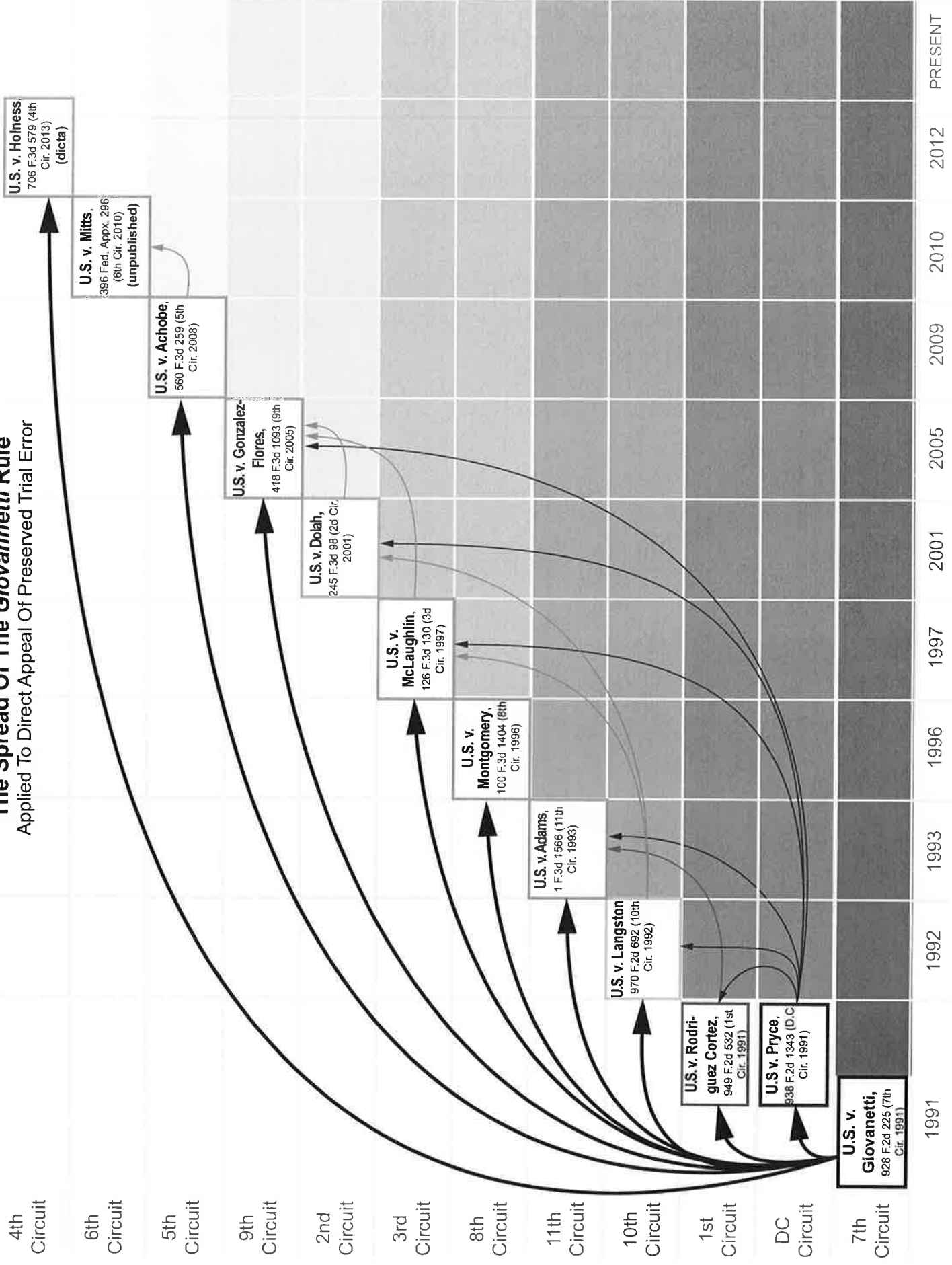
“(1) IN GENERAL.—Each application for an order under this section shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under subsection (a)(1). Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements of such application, as set forth in this section, and shall include—

“(A) the identity of the Federal officer making the application;

“(B) the identity, if known, or a description of the United States person who is the target of the acquisition;

“(C) a statement of the facts and circumstances relied upon to justify the applicant's belief that the United States person who is the target of the acquisition is—

The Spread Of The *Giovannetti* Rule Applied To Direct Appeal Of Preserved Trial Error



UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FILED

MAR 16 2017

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MOHAMED OSMAN MOHAMUD,

Defendant-Appellant.

No. 14-30217

D.C. No. 3:10-cr-00475-KI-1
District of Oregon,
Portland

ORDER

Before: PREGERSON, BEA, and OWENS, Circuit Judges.

The panel has voted to deny the petition for panel rehearing. Judges Bea and Owens voted to deny the petition for rehearing en banc, and Judge Pregerson so recommends.

The full court has been advised of the suggestion for rehearing en banc, and no active judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for panel rehearing and the petition for rehearing en banc are therefore DENIED.

No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

MOHAMED OSMAN MOHAMUD,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To
The United States Court Of Appeals For The Ninth Circuit

CERTIFICATE OF SERVICE AND MAILING

I, Stephen R. Sady, counsel of record and a member of the Bar of this Court, certify that pursuant to Rule 29.3, service has been made of the within PETITION FOR WRIT OF CERTIORARI on the counsel for the respondent by hand-delivery on June 14, 2017, an exact and full copy thereof addressed to:

Ryan W. Bounds
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

Ethan D. Knight
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

Pamala R. Holsinger
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

Kelly A. Zusman
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

and by depositing in the United States Post Office, in Portland, Oregon on June 14, 2017, first class postage prepaid, an exact and full copy thereof addressed to:

Patrick C. Toomey
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

John D. Cline
Law Office of John D. Cline
235 Montgomery Street
San Francisco, CA 94104

Joseph F. Palmer, Esquire
U.S. Department of Justice
Rm 1250
950 Pennsylvania Ave., N.W.
Washington, DC 20530

Jeffrey B. Wall
Acting Solicitor General of the U.S.
Room 5614
Department of Justice
950 Pennsylvania Avenue, N. W.
Washington, DC 20530-0001

Further, the original and ten copies were mailed to the Honorable Scott S. Harris, Clerk of the United States Supreme Court, by depositing them in a United States Post Office Box, addressed to 1 First Street, N.E., Washington, D.C., 20543, for filing on this 14th day of June, 2017, with first-class postage prepaid.

Dated this 14th day of June, 2017.



Stephen R. Sady
Attorney for Petitioner

Subscribed and sworn to before me this 14th day of June, 2017.



Notary Public of Oregon



No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

MOHAMED OSMAN MOHAMUD,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To
The United States Court Of Appeals For The Ninth Circuit

CERTIFICATE OF SERVICE AND MAILING

I, Stephen R. Sady, counsel of record and a member of the Bar of this Court, certify that pursuant to Rule 29.3, service has been made of the within PETITION FOR WRIT OF CERTIORARI, modified to include references on pages ii and 2 to the added denial of rehearing and rehearing en banc at page 130 of the Appendix, on the counsel for the respondent by hand-delivery on July 5, 2017, an exact and full copy thereof addressed to:

Ryan W. Bounds
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

Ethan D. Knight
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

Pamala R. Holsinger
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

Kelly A. Zusman
Assistant U.S. Attorney
Suite 600
1000 S.W. Third Avenue
Portland, OR 97204

and by depositing in the United States Post Office, in Portland, Oregon on July 5, 2017, first class postage prepaid, an exact and full copy thereof addressed to:

Patrick C. Toomey
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004

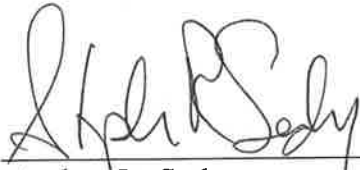
John D. Cline
Law Office of John D. Cline
235 Montgomery Street
San Francisco, CA 94104

Joseph F. Palmer, Esquire
U.S. Department of Justice
Rm 1250
950 Pennsylvania Ave., N.W.
Washington, DC 20530

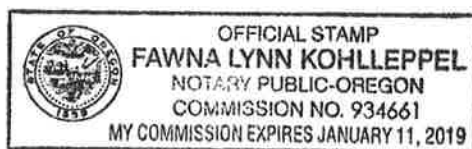
Jeffrey B. Wall
Acting Solicitor General of the U.S.
Room 5614
Department of Justice
950 Pennsylvania Avenue, N. W.
Washington, DC 20530-0001

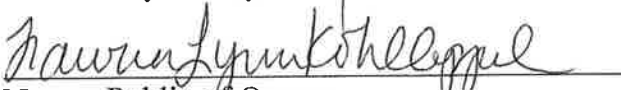
Further, the original and ten copies were mailed to the Honorable Scott S. Harris, Clerk of the United States Supreme Court, by Federal Express, addressed to 1 First Street, N.E., Washington, D.C., 20543, for filing on this 5th day of July, 2017, with first-class postage prepaid.

Dated this 5th day of July, 2017.


Stephen R. Sady
Attorney for Petitioner

Subscribed and sworn to before me this 5th day of July, 2017.




Notary Public of Oregon