Stephen R. Sady
Chief Deputy Federal Public Defender
steve_sady@fd.org
Steven T. Wax
Federal Public Defender
steve_wax@fd.org
Lisa Hay
Assistant Federal Public Defender
lisa_hay@fd.org
101 S.W. Main Street, Suite 1700
Portland, Oregon 97204
503-326-2123 Telephone
503-326-5524 Facsimile

Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**Case No. 3:10-cr-00475-KI**
Plaintiff,	**REPLY TO GOVERNMENT'S UNCLASSIFIED RESPONSE TO DEFENDANT'S ALTERNATIVE MOTION FOR SUPPRESSION OF EVIDENCE AND NEW TRIAL**
v.	
MOHAMED OSMAN MOHAMUD,	
Defendant.	

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

FEDERAL CASES

FEDERAL STATUTES

MISCELLANEOUS

Introduction

The government's response asks the Court to approve a radical expansion of the power of government agents to read and listen to Americans' electronic communications without a warrant or any other form of individualized judicial review. The government's innovative claims include:

- The Warrant Clause is not implicated by electronic surveillance of Americans' communications, whether at acquisition, retention, accessing, or use, as long as the original, nominal target is a non-United States person abroad;

- The massive acquisition, databasing, querying, and use of Americans' communications, even though an inevitable concomitant of the government's program, are merely "incidental" and therefore receive no protections under the Fourth Amendment;

- The Fourth Amendment should have an exception that allows mass acquisition of Americans' electronic communications for subsequent retention and accessing, all without any individualized judicial review.

The government's claim that Americans lack any meaningful privacy interest in their international electronic communications, which permits government agents to rummage through and read Americans' emails and listen to their phone calls without restriction, would result in a stunning and unjustified depreciation of American freedom.

No precedent approves the massive scope of the government's acquisition of Americans' communications or the government's claims that the Fourth Amendment's protections are inapplicable once communications have been acquired.[1] No precedent allows the government to inspect the contents of millions of American communications simply because they might relate to

[1] The defense understands that telephone calls and emails are intercepted under § 702 of the FISA Amendments Act (FAA). The electronic surveillance should be understood to incorporate similar communications such as text messages, instant messaging, and online direct communications such as Skype, to the extent such electronic communications are being intercepted under § 702.

the "foreign affairs" of the United States. No precedent allows government agents to retain, database, query, listen to, read, and disseminate the most private of communications of United States citizens, even though they are written and sent from homes in the United States, simply because the communication were acquired by the government's dragnet for information. The courts have yet to countenance such an Orwellian world.

The government claims the Court cannot consider a facial challenge to the statute and that, with the defense blindfolded as to the statute's application, the Court can only consider the statute as applied. CR 509 at 4. Not so. The federal courts routinely consider facial challenges, just as from the day of enactment, the FAA has been challenged in the litigation leading to *Clapper v. Amnesty U.S.A.*, 133 S. Ct. 1138 (2013). On its face, the Court can strike down the FAA for several reasons:

- under the Fourth Amendment, as in the electronic surveillance statute in *Berger v. New York*, 388 U.S. 41, 44 (1967), "the language of the statute is too broad in its sweep," failing to implement the minimal safeguards to prevent warrantless, unreasonable searches and seizures of Americans' electronic communications;

- under the First Amendment, the statute's facial breadth and vagueness chill the exercise of rights by millions of Americans in their use of electronic communications;

- under the separation of powers, § 702 institutionalizes an administrative, law-making role for judges that violates Article III of the Constitution and undermines judicial neutrality.

The statute also violates the Constitution as applied, as the known programs instituting § 702 fail to satisfy Fourth Amendment requirements. The vast amount of redacted material in the government's brief prevents the defense from fully presenting, and the Court from fully considering, the ways in which the statute as applied violates constitutional rights. This limitation infringes on

the due process right to notice and a fair opportunity to be heard. Because the FAA program intrudes upon core privacy interests, without any meaningful counter-balancing protections, the Court should find that § 702 of the FAA, on its face and as applied, violates the protections found in the First and Fourth Amendments and the constitutionally-based separation of powers doctrine.

Alternatively, the Court could construe the statute in a limiting manner that would avoid serious constitutional questions. Such a construction should foreclose the current surveillance programs implemented by the government under § 702, requiring suppression of evidence obtained or derived from the violation of the properly construed statute. *See Zadvydas v. Davis*, 533 U.S. 678 (2001) (serious constitutional problems with indefinite detention statute warranted interpretation to limit detention to six months).

In the event the foregoing analyses do not lead to suppression of evidence in this case, the Court must determine whether the surveillance exceeded the scope of the programmatic authorizations. If the surveillance was not lawfully authorized or conducted, the Court should order suppression of all information obtained and derived from the warrantless surveillance under 50 U.S.C. § 1806(g) and the constitutionally-based exclusionary rule.

A. The Mass Acquisition, Retention, And Accessing Of American Citizens' Electronic Communications Under § 702 Of The FISA Amendments Act Violates The Fourth Amendment.

This case involves government agents in the United States searching and seizing the private electronic communications of American citizens who are living in the United States. The government claims that the Warrant Clause is irrelevant, and that the privacy intrusions on Americans are reasonable because the Fourth Amendment does not protect foreigners who do not live in America. But, regardless of the nominal targeting of foreign persons abroad, the § 702

programs routinely acquire huge numbers of American communications in America. The mass acquisition of American communications – let alone the retention, use, and later querying and accessing of those communications – implicates 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. The constitutional protections for Americans' privacy are not so feeble.

Section 702 fails at every level of Fourth Amendment analysis. First, the extreme intrusion into the core privacy rights of Americans should require a warrant or a similar, individualized judicial review. Second, even if a narrow, foreign intelligence exception to the warrant requirement exists, the § 702 programs do not fit within such an exception. Finally, to the extent that "reasonableness" is at issue, the § 702 surveillance programs are unreasonable based on the competing interests at stake and the lack of any meaningful protection for Americans' communications.

1. The Warrant Requirement Applies To Government Surveillance Of The Electronic Communications Of American Citizens Living In The United States.

The government claims the measure for constitutional protections of American citizens, whose communications are listened to and read under § 702, is that of foreign persons who are searched abroad – nothing. CR 509 at 27. Relying on a case involving a search of property in Mexico owned by a nonresident alien, the government asserts that, because § 702 aims at foreigners abroad, the Fourth Amendment is inapplicable. CR 509 at 27-28 (citing *United States v. Verdugo-Urdiquez*, 494 U.S. 259 (1990)). However, the government's premise ignores that the sweep of the programs operated under § 702 inevitably and inexorably results in the search and seizure of massive

amounts of Americans' private communications. Because Americans retain an undiminished expectation of privacy in their electronic communications, the Fourth Amendment's Warrant Clause applies.

a. The § 702 Programs Inevitably Result In The Massive Collection, Retention, And Accessing Of Americans' Communications.

The government's response is based throughout on its assertion that its seizures and searches of Americans' communications should be of no concern to the Court because they are merely "incidental" to the legitimate seizure of the communications of targeted foreigners. CR 509 at 4, 10, 21, 23, 24, 26-30, 32, 40, 41, 43, 47, 50, 54, 59, 64, 71, 89. The seizure and search of Americans' communications are anything but incidental; they are extensive, pervasive, and inherent to the government's search and seizure program. The government seizes hundreds of millions of communications per year under § 702. CR 503 at 5-6, 8. Of these seizures, many involve American citizens. Even if only one percent involved American communications, that would result in 2.5 million communications every year. To call that potential volume of seizures "incidental" smacks of Orwellian doublespeak.

In down-playing the extent of intrusion into the privacy of Americans, the government highlights a Microsoft "disclosure report" that states the company received "fewer than 1000 FISA orders" that involved 16,000 to 16,999 user accounts in a six month period. CR 503 at 62 n.43. However, the suggestion that the Microsoft data means that the government does not engage in "bulk 'dragnet' surveillance" is misleading and incorrect. *Id*. With respect to the "dragnet" aspect, the government appears to entirely ignore its § 702 Upstream program, which indiscriminately searches

all internet communications travelling along surveilled sections of the "Internet Backbone." CR 503 at 9.[2]

With respect to the "bulk" aspect, the government's citation to a single email provider out of the hundreds of such providers in the United States – from major providers such as Google, Apple, AT&T, Comcast, and Yahoo to the myriad of minor, regional providers – does not reflect the massive amount of communications being seized and retained in government databases. Even extrapolating just from the government's single citation, the number of communications involved are immense. Assuming conservative estimates of 32,000 user accounts surveilled per year, with each account sending only five emails per week, the government would seize over six million communications yearly from a single email provider.

In addition, the number of email users whose communications were seized is far greater than the number of accounts subject to orders because it includes every user and email account with which the subject account communicated. In some cases, it would also include every email user communicating "about" a subject account.

Guesswork is to some extent unnecessary because the FISC has provided some relevant numbers, a fact entirely missing from the government's discussion. In 2011, Judge Bates wrote in a now-declassified opinion that the "NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702." *[Case Name Redacted]*, [docket number

[2] This is apparently not the first time that the government has neglected to acknowledge the Upstream program – and "about" collections – in regard to FAA litigation. Charlie Savage, *Justice Dept. Criticized on Spying Statements*, N.Y. Times, May 13, 2014 (describing letter from Senators Ron Wyden and Mark Udall to the DOJ objecting to omissions regarding the scope of § 702 collections before the Supreme Court in *Clapper*).

redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011). Assuming four years of warrantless surveillance between the passage of the FAA and the 2011 opinion, the government would have seized something on the order of *one billion* internet communications alone.[3] Given these staggering numbers, the government's reliance on Microsoft's report to refute the notion of "bulk" collection should be rejected. These are hardly de minimus intrusions. *Id*. at *26 (emphasis in original) (While noting that the percentage of communications seized that intruded on protected interests was relevant, the court stated that it "must also take into account the absolute number of non-target protected communications that are acquired," finding that "tens of thousands of non-target protected communications is a *very* large number.").

Because the government seeks to justify the legality of § 702 seizures based, in part, on the extent of intrusion on the privacy of Americans, and seeks to minimize the extent of that intrusion, an evidentiary hearing on that issue would be appropriate. As recognized by the FISC, if that number is even a fraction of one percent (a number the government suggested in its memorandum at CR 509 at 62 n.43), it would be "very large" in absolute terms. As argued in the defense opening memorandum and below, evidentiary development can be effectively accomplished only in an adversary proceeding.

[3] The FISC opinion did not address telephone or other non-internet based acquisitions. Presumably, the total number of electronic communications seized yearly is significantly greater than 250 million.

b. The Mass Collection Of Americans' Electronic Communications Aimed At Overseas Targets Greatly Exceeds Previous Programs With Fewer Protections For Citizens.

In the opening memorandum, the defense presented a chart demonstrating the lack of § 702 protections when compared to traditional FISA and Article III electronic surveillance. CR 503 at 7. The government does not controvert the disparate protections, instead relying on *In re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008). In *Directives*, the FISA Review Court addressed the Protect America Act of 2007 (PAA) against claims by a service provider that the program violated the Fourth Amendment. Contrary to the government's claim, the court's reasoning does not support the constitutionality of § 702.

First, the government ignores the *Directives* case's adherence to the Warrant Clause as providing the lodestar for Fourth Amendment reasonableness. 551 F.3d at 1013 ("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.") (citing *In re Sealed Cases*, 310 F.3d 717, 737, 742 (FISA Ct. Rev. 2002)). Similarly, the Supreme Court referenced legislative design based on the "type" of protections afforded under the Warrant Clause. *United States v. U.S. Dist. Court for the E. Dist. Of Mich.*, 407 U.S. 297, 322-23 (1972) (*Keith*). For that reason, the defense analyzed in the opening memorandum each of the constituent protections assured by the Warrant Clause and the absence of any meaningful analogue under § 702. CR 503 at 13-28. In stark contrast, the government does not even attempt to claim that § 702 provides parallel protections. Instead, ignoring the language in the prime case upon which it relies, the government suggests the Warrant Clause is irrelevant and that protections for American citizens' telephonic and email communications are as non-existent as those of foreigners living and communicating abroad.

Second, the government ignores the fundamental distinctions between the PAA and the FAA's § 702. In *Directives*, the court cautioned that "our decision does not constitute an endorsement of broad-based, indiscriminate executive power." 551 F.3d at 1016. Due to "several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions," the court ultimately rejected the service providers objections. *Id*. However, some of the most critical safeguards present in the PAA, and relied on by the court, are absent from § 702. For example, the PAA apparently did not involve retention, databasing, and later accessing of incidentally collected electronic communications:

> The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.

551 F.3d at 1015. In this case, by contrast, the information can be put in a database for later access and review of content.[4] The government claim that, once Americans' communications are "incidentally" acquired, the Fourth Amendment is not implicated is one of the most egregious departures from traditional Fourth Amendment protections wrought by the § 702 program.

A second major difference between the PAA and § 702 is that the former has at least an executive determination of probable cause. Specifically, the PAA incorporated § 2.5 of Executive Order 12333, which required the Attorney General to determine on a case-by-case basis whether there was probable cause to believe the target of the surveillance was a foreign power or an agent

[4] The intelligence community asserts without qualification that "subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody." PCLOB Hearing at 28 (Mar. 19, 2014). As testified to at the PCLOB hearing, the government is later querying the databases derived from FAA activity with specific United States person identifiers.

of a foreign power. *Id*. at 1014. Thus, the PAA provided some level of individualized suspicion similar to that which exists under traditional FISA surveillance, albeit the determination was made by the Executive Branch rather than a judicial officer. In contrast, § 702 requires no probable cause determination of any kind by any branch of the government.[5]

It is also important to note that the facts before the courts in the cases relied on in *Directives* bear no relation to the facts before this Court. In *United States v. Kahn*, 415 U.S. 143 (1974), the question was whether the conversations of Minnie Kahn could be used when they were seized pursuant to a court authorized Title III wiretap for a particular telephone and conversations of Irving Kahn and "others as yet unknown." Upholding a judicially authorized warrant to intercept all calls involving a telephone known to be used for illegal purposes is not the type of "incidental" seizure at issue in this case, if it is "incidental" at all. Similarly, *United States v. Schwartz*, 535 F.2d 160 (2nd Cir. 1976), also involved a judicially approved Title III wiretap. Schwartz was overheard on two of the calls intercepted. The calls were permitted to be used against him because "the extent of non-pertinent matters was slight. It is virtually impossible to completely exclude all irrelevant matter from intercepted conversations." *Id*. at 164. Here, in contrast, the government activity was not based

[5] Even the much criticized warrantless surveillance program authorized by President Bush after the 9/11 attacks prior to the passage of the PAA had a narrower focus than the FAA. In that program, surveillance could only occur after an executive determination that there was a reasonable basis – which the Attorney General in 2006 equated with the traditional probable cause standard – "that one party to the communication [wa]s a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." 1 David S. Kris & J. Douglas Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, § 15:13 (2d ed. 2012). Section 702 requires no similar determination regarding an individual or any limitation based on a nexus between the warrantless surveillance and a threat to the United States.

on probable cause, there was no judicial authorization, and the extent of seizure of protected persons calls was massive.

To the extent the service provider in *Directives* failed to raise issues, such as First Amendment and separation of powers claims, the decision does not carry persuasive value.[6] Further, the hypothetical problems raised by the service provider in *Directives* failed to account for the individual interests at stake under the concrete facts of this case. The government's reliance on *Directives* ignores the passages that support suppression in this case, while exaggerating the endorsement of unreviewed executive authority in a case that cautioned that "the Constitution is the cornerstone of our freedoms, and government cannot unilaterally sacrifice constitutional rights on the altar of national security." 551 F.3d at 1016.

c. Both The Identity Of The United States Citizen And His Location In The United States Foreclose Loss Of Privacy Rights.

The government attempts to treat an American citizen living in the United States as within the scope of *Verdugo-Urquidez*'s holding that a Mexican citizen, whose property was seized in Mexico, does not have rights under the Fourth Amendment. CR 509 at 31-32. The core of the Court's reasoning in that case confirms that, as an American citizen, the defendant in this case is fully protected by the Constitution: "the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory." 494 U.S. at 266. The Court also found significant the location of the

[6] "Constitutional rights are not defined by inferences from opinions which did not address the question at issue." *Texas v. Cobb*, 532 U.S. 162, 169 (2001).

search: "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." *Id*. at 274-75.

In contrast, the present case involves a United States citizen living in Beaverton, Oregon. The government admits that the location of the search is in the United States: "collection under Section 702 takes place within the United States." CR 509 at 31. When the government claims that, contrary to the direct reasoning of *Verdugo-Urquidez*, the location of the search "makes no difference" (CR 509 at 31), the only support cited is *United States v. Yonn*, 702 F.2d 1341 (11th Cir. 1983). In *Yonn*, agents in the United States made consensual recordings of a conversation between an informant and a drug dealer that took place in a motel room. The court found no significance in the location of the microphone in the motel room, which was activated only when the informant was in the room and the recording was therefore consensual: "The location of the electronic equipment does not alter the irrefutable fact that Yonn had no justifiable expectation of privacy in his conversation with Dozier." 702 F.2d at 1347. *Yonn* simply provides no support for the warrantless, non-consensual intrusion by government agents into the private communications of American citizens in the United States.

2. The FAA Program Does Not Fit Into Any Foreign Intelligence Exception To The Warrant Requirement Because The Searches And Seizures Are Not Narrowly Circumscribed, Protective Of Americans' Privacy, Or Individually Subject To Fourth Amendment Protections.

The government's claim regarding a foreign intelligence exception both incorrectly frames the question and incorrectly limits its potential scope. CR 509 at 32. The government recognizes that, as the FISC has noted, "[t]here surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable." *Id*. (citing *[Case Name Redacted]*,

2011 WL 10945618, at *26). The present case presents exactly such circumstances. But the question does not only apply to the mass "collection" of American communication; what the government does with acquired American communications thereafter separately falls outside any exception to the warrant requirement. Here, the Court should find that no foreign intelligence exception applies to the overbroad surveillance authorized by, and carried out under, § 702.

a. The "Special Needs" Doctrine Does Not Apply To Mass Acquisition, Retention, And Accessing Of Americans' Electronic Communications.

The government's invocation of "special needs" fails to recognize that the § 702 does not on its face invoke or justify mass surveillance of American communications. CR 509 at 32-33. The reason the Snowden disclosures regarding the FAA programs produced shock waves throughout the country was that the statute did not provide any notice or explicit authorization for acquisition, retention, processing, accessing, and dissemination of the contents of American communications. Programmatic 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, as in *Ferguson v. City of Charleston*, where the Court remanded to assure that, after "close review," the drug-testing program of pregnant women was primarily directed toward health issues. 532 U.S. 67, 81, 84-85 (2001); *see also Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995) (school locker searches for drugs primarily addressed safety and health issues). Similarly, the probation and parole search cases involve individuals with substantially reduced privacy expectations as a result of criminal convictions with the primary purpose being supervision. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001); *see also Maryland v. King*, 133 S. Ct. 1958 (2013) (reduced privacy for persons arrested allowed for DNA testing). In contrast, the FAA

explicitly disclaims a primary purpose of foreign intelligence gathering and purports to authorize programmatic acquisition, retention, and accessing merely based on a "significant purpose" of collecting foreign intelligence. 50 U.S.C. § 1881a(g)(2)(A)(5).

Because the FAA targeting need not be "primarily" for foreign intelligence, the risk of overbroad collection and bleed-over into criminal investigations is especially high. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 40-42 (2000) (highway checkpoints unconstitutional based on their "primary purpose" of drug interdiction). Because foreign intelligence need not be the "primary purpose" of the § 702 programs, but merely a "significant purpose," the "special need" doctrine should not apply. *Edmond*, 531 U.S. at 48 ("Nor does our opinion speak to other intrusions *aimed primarily at purposes* beyond the general interest in crime control.") (emphasis added); *Ferguson*, 532 U.S. at 81 ("In looking to the programmatic purpose, we consider all the available evidence in order to determine the relevant *primary purpose*.") (emphasis added). Further, the government has made no showing regarding the inability to provide a measure of judicial oversight regarding the acquisition of American communications and the incremental intrusions of retaining, processing, querying, using, and disseminating Americans private electronic communications.

Although some courts have invoked "special need" by analogy in support of a foreign intelligence exception to the Warrant Clause, the present case does not support invocation of a doctrine that, if not carefully cabined as in *Ferguson* and *Edmond*, threatens to swallow the Fourth Amendment. *See Edmond*, 531 U.S. at 451 ("individualized suspicion of wrongdoing" is the "usual rule"). This danger is especially acute in the present case where, with no clear statutory authorization, secret government agencies seize and read massive amounts of Americans' private communications with no requirement that the primary purpose of the acquisition, retention, and

accessing relates to national security, as opposed to diluted information related to "the conduct of foreign affairs of the United States," which could include a universe of innocuous information about trade, social matters, politics, religion, and more. *Compare* 50 U.S.C. § 1801(e)(1) *with* 50 U.S.C. § 1801(e)(2). At the very least, the government's invocation of "special needs" strongly supports adversary proceedings. *Ferguson*, 532 U.S. at 81 (requiring "close review" of the "scheme at issue" in determining the need in question was not "special, as that term has been defined in our cases.") (citing *Chandler v. Miller*, 520 U.S. 305, 322 (1997)).

b. Any Foreign Intelligence Exception To The Warrant Requirement Must Be Narrowly Construed.

The government's response ignores the abundant authority cited by the defense that the scope of any foreign intelligence exception must be closely circumscribed, as are all warrant exceptions. *See Gant v. Arizona*, 556 U.S. 332, 338 (2009) (describing warrant exceptions as "specifically established and well delineated") (citations omitted); *Georgia v. Randolph*, 547 U.S. 103, 109 (2006) (describing exceptions as "jealously and carefully drawn") (citation omitted). Although the government claims the exception is not "narrow," CR 509 at 35, cases the government relies upon are to the contrary: "the warrant exception adopted by this Court is narrowly drawn to include only those overseas searches, authorized by the President (or his delegate, the Attorney General), which are conducted primarily for foreign intelligence purposes and which target foreign powers or their agents." *United States v. Bin Laden*, 126 F.Supp.2d 264, 277 (S.D.N.Y. 2000) (citing *United States v. Truong*, 629 F.2d 908, 915-17 (4th Cir. 1980)). Instead, the government invokes foreign national security to make the blanket claim that no judicial warrant is required and disdains to demonstrate how any analogue to the protections of the Warrant Clause are included in § 702.

The government criticizes the defense for its "misplaced" reliance on *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), without acknowledging that the very cases upon which the government relies in its response refer to *Keith* as providing the template for Fourth Amendment analysis of foreign intelligence surveillance. *See*, *e.g.*, *Sealed Cases*, 310 F.3d at 738 ("Congress was aware of *Keith*'s reasoning, and recognized that it applies a fortiori to foreign threats."); *Truong*, 629 F.2d at 913 (the Supreme Court in *Keith* "formulated the analytical approach we employ here in an analogous case"). The Court's reasoning in *Keith* should inform this Court's analysis, especially because Congress directly and explicitly considered the case in enacting FISA. *See*, *e.g.*, S. Rep. 604(I), 95th Cong., 1st Sess. 13-14, *reprinted* in 1978 U.S.C.C.A.N. 3904, 3914-16; S. Rep. 701, 95th Cong., 1st Sess. 9, 15-16, *reprinted* in 1978 U.S.C.C.A.N. 3973, 3977, 3984-85.

Congress was not only aware of the Court's articulation of the range of privacy interests that are necessary to our constitutional democracy, the Church Committee Report had just warned that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature." S. Rep. No. 94-755 (Book II), at 2 (1976). This case involves domestic investigative activities to gather foreign intelligence: searches and seizures of the private communications of an American citizen, sent and received in the United States, that occurred in the United States. The reasoning of *Keith* is directly relevant. Indeed, the constitutional considerations favoring privacy are weightier because the breadth of surveillance of "foreign intelligence purposes," as defined in the FAA broadly include any information relevant to "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2)(B).

The cases upon which the government relies involve limitations completely missing from the § 702 programs. For example, in citing to *Truong*, the government omits the central holding that cabins warrantless surveillance in a manner that § 702 completely disregards. 629 F.2d at 915 (the Executive Branch should be excused from securing a warrant "*only* when the surveillance is conducted 'primarily' for foreign intelligence reasons" and when "the object of the search or the surveillance is a foreign power, its agents or collaborators") (emphasis added). Similarly, in *Sealed Cases*, the FISA Review Court, in conducting an ex parte review of whether the FISC inappropriately created a "wall" between national security investigation and national security crimes, focused on the narrow scope of the foreign intelligence surveillance. The FISA court had to find "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power, meaning a group engaged in international terrorism or activities in preparation for terrorism." 310 F.3d at 722; *see Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir 1975) (en banc) (absent exigent circumstances, foreign national security electronic surveillance of domestic individuals, who were neither agents of nor acting in collaboration with a foreign power, required a judicial warrant).

Moreover, the surveillance in *Sealed Cases* only related to potential attack, sabotage, and clandestine intelligence activities under 50 U.S.C. § 1801(e)(1), explicitly discounting reliance on information gathering related to "the conduct of the foreign affairs of the United States" under 50 U.S.C. § 1801(e)(2). 310 F.3d at 722-23. The Court distinguished between "protective" or "counterintelligence" information at issue in § 1801(e)(1) and the general information referred to as "affirmative" or "positive" in § 1801(e)(2). *Id*. at 722 n.9. *Sealed Cases* only involved the national security issues in § 1801(e)(1); the authorizations under the FAA include foreign affairs information

that may involve no danger and is virtually limitless. Any foreign intelligence exception to the Warrant Clause is far narrower than the massive programmatic collection and accessing of targets, who are extraordinarily broadly defined, for purposes that are extraordinarily broadly defined, resulting in the massive searches of Americans' private communications.

Finally, the government relies on a case involving random and suspicionless subway baggage searches in New York City that, like airport searches, had as their purpose protection against terrorist attack. *MacWade v. Kelly*, 460 F.3d 260 (2d Cir. 2006). Subway customers were given the option of submitting to the search or leaving the subway. In contrast, § 702 involves the massive *secret* collection of American communications that only has a "significant purpose" of general gathering of information about foreign policies issues. Any foreign intelligence exception to the Warrant Clause must be limited to actions designed to protect against foreign threats to the national security, and not to allow surveillance of Americans for general information-gathering about foreign policies. The government fails to describe a foreign intelligence surveillance exception that is sufficiently narrow to avoid the destruction of privacy interests precluded by the Court's reasoning in *Keith*.

c. The Purposes Of § 702 Surveillance Do Not Diminish Americans' Protected Privacy Rights And Does Not Justify Warrantless Search And Seizures.

There is no disagreement that electronic surveillance under § 702 "goes beyond routine law enforcement." *Compare* CR 503 at 17, *with* CR 509 at 37. However, the multiple purposes do not reduce the protected privacy interests of American citizens, nor do they provide carte blanche for the government to intrude on those interests merely by reference to some non-law enforcement purpose.

The government's citation to *Cassidy v. Chertoff*, 471 F.3d 67 (2d Cir. 2006), a decision authored by now-Justice Sotomayor, supports the need to rigorously assess programmatic intrusions

in the name of national security. In *Cassidy*, Justice Sotomayor addressed the propriety of limited warrantless screenings of passenger baggage and vehicles on certain maritime vessels. In light of the September 11, 2001, terrorist attacks, and pursuant to the Maritime Transportation Security Act of 2002, the Coast Guard assessed the "risks associated with specific threat scenarios" against particular types of vessels. *Cassidy*, 471 F.3d at 70-71. This assessment focused directly on the threat of terrorism: "the likelihood that a particular type of vessel would be a terrorist target or would be used as a weapon itself; the plausibility of terrorists actually carrying out various hypothetical attack scenarios; the risk associated with a given attack against a given target; and the likelihood and consequences of various attack scenarios." *Id*. at 71. As a result of that assessment, certain large vessels were deemed to be "at a high risk of a transportation security incident," which led to "minimally intrusive" random "visual inspections of vehicles and their trunks and brief examinations of the contents of carry-on baggage." *Id*. at 71, 78-79. Further, similar to previously approved airport screening measures, passengers were provided "[a]mple notice" of the potential for warrantless searches prior to attempting to board a particular vessel. *Id*. at 79.

Two points in *Cassidy* are relevant here. First, the clear non-law enforcement purpose of preventing specific terrorist attacks did not diminish the passengers' "full expectation of privacy." *Cassidy*, 471 F.3d at 76-77. Second, Justice Sotomayor stressed the "very narrow circumstances" of the case and the "obvious nexus" between the "minimally intrusive searches" and "protecting a ferry" from terrorist attack. *Id*. at 78 n.4, 82. In other words, it was important that even these minimal intrusions into privacy interests be justified by narrow and specific non-law enforcement purposes. Justice Sotomayor noted the "legitimate concern" of a slippery-slope "because the threat of terrorism is omnipresent" and there is thus "no clear limit to the government power to conduct

suspicionless searches." *Id*. at 80. These concerns were not implicated in *Cassidy*, however, because the government "imposed security requirements only on the nation's largest ferries after making extensive findings about the risk these vessels present in relation to terrorism and . . . the scope of the searches [wa]s rather limited." *Id*. at 81.

Section 702 surveillance slides down the slippery-slope to complete sacrifice of American privacy for only nebulous purposes related to foreign affairs. In contrast to the open and announced cursory searches when boarding certain maritime vessels in *Cassidy*, the surreptitious intrusions on American's private communications under § 702 are far more substantial, potentially including (1) any communications that cross borders (including wholly domestic communications that happen to cross a border (CR 509 at 14)); (2) any communication with or about a foreign individual abroad; (3) any communication (including wholly domestic ones) traversing the Internet "backbone"; and (4) any communication (including wholly domestic ones) that happens to travel in the same Internet "packet" as a targeted one. Additionally, despite the government's repeated invocation of terrorism concerns, § 702 has no such limited nexus because the definition of "foreign intelligence" includes information generally related to "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2)(B). Thus, even though § 702's purpose extends beyond ordinary law enforcement, it also has a purpose far broader than combatting terrorism. Given the undiminished privacy interests of Americans in this context, the purpose invoked by the government here is insufficient to justify sweeping warrantless surveillance.

d. The Government's Claim That Providing Fourth Amendment Protections Would Be Inconvenient Neither Justifies Abandonment Of Traditional Privacy Guarantees Nor Finds Support In The Record.

Given that § 702's purpose is far broader than preventing imminent terrorist attacks – or anything related to terrorism at all – the government's blanket assertion that additional Fourth Amendment protections are "impracticable" is unsupported. CR 509 at 38. Nor is impracticability a ground to abandon constitutional rights. Even in situations where the government legitimately must act quickly to thwart terrorism, or otherwise deal with a threat to national security, there are ways to accomplish that goal without completely subverting the privacy interests of Americans.

When the government seeks to marginalize the Constitution on grounds of efficiency and practicality, the liberty of all citizens is jeopardized:

> Cases like this involve grave danger. The very natural desire of government officers who try to enforce the law to the best of their ability leads them to adopt the most practical and efficient way to do it whenever by some plausible reasoning they can satisfy themselves that no constitutional rights are contravened. But their zeal for the cause in which they have enlisted so often creates in their minds such an emphasis upon the theory that the virtue in the end will justify the means that the fundamental rights of a liberty loving people will be gradually sapped, undermined, and finally destroyed by a subtle, insidious, and persistent narrowing of vital bedrock principles unless courts are steadfast and firm in the preservation of what has been gained through centuries of struggle. The Fourth Amendment, which prohibits unreasonable searches and seizures, is one of the pillars of liberty so necessary to a free government that expediency in law enforcement must ever yield to the necessity for keeping the principles on which it rests inviolate.

United States v. 1013 Crates Of Empty Old Smuggler Whiskey Bottles, 52 F.2d 49, 50-51 (2d Cir. 1931). The Supreme Court has echoed those sentiments in the very context of electronic surveillance:

> In any event we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement . . . . Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that without the use of

> such devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and – what is more important – without attending illegality.

Berger v. New York, 388 U.S. 41, 62-63 (1967). In short, efficiency is not a valid reason to dispense with constitutional protections.

The concerns expressed in the above two quotations are amplified in the national security context where even more zeal may exist than in traditional law enforcement, and where the actions of the Executive Branch are often hidden from public scrutiny. One only need consider the Snowden disclosures and the public outcry that followed, or even the failure to provide the statutorily required notice of § 702 activity in this very case, to recognize how difficult it is to meaningfully learn about and review actions taken in the name of national security that threaten to undermine constitutional protections. As a result, when such activities do come to light, it is critical that the government's invocation of practicality and need receive meaningful scrutiny.

Here, the government's argument about practicality and need are factually deficient for several reasons. First, the government's claim that judicial oversight of warrantless searches and seizures of Americans' communications under § 702 would "hinder the government's ability to monitor fast-moving threats" ignores the fact that Congress has already dealt with this concern in the context of traditional FISA surveillance. CR 509 at 39. Under 50 U.S.C. § 1805(e), Congress provided an exception for exigent circumstances whereby the Executive could engage in individualized surveillance on an emergency basis, then later receive approval from the FISC. The government provides no reason why a similar arrangement could not be applied in the context of § 702 surveillance.

Second, the government – as it does throughout its brief – focuses only on the acquisition stage without addressing whether it is equally "impracticable" to provide Fourth Amendment protections to seized American communications at another stage. For example, the government could be required to seek judicial authorization before it retains, disseminates, or queries already seized American communications, which is essentially the current procedure under a different section of FISA. 50 U.S.C. § 1801(h)(4). In fact, judicial approval prior to querying is now what occurs for § 215 metadata collection, although the government originally raised many of the same objections that it raises here. *Klayman v. Obama*, 957 F. Supp. 2d 1, 39-40 (D.D.C. 2013) (questioning government justifications for § 215); White House Press Release, *Statement by the President on the Section 215 Bulk Metadata Program* (Mar. 27, 2014) (requiring judicial approval for § 215 queries). The government could use a wide range of traditional and technological screens to interpose some judicial judgment between government agents and Americans' communications. No such potential system can be evaluated because § 702 provides nothing in the way of individualized review before Americans' communications are listened to and read.

Third, surveillance under § 702 does not limit the collection or retention of Americans' private communications to only those involving terrorism or other similar threats to national security. Although the government's brief almost exclusively discusses "threats," "terrorist groups," and other concerns "vital to the Nation's security," § 702 allows the government to collect and retain communications that have nothing to do with any danger to the country. *See* 50 U.S.C. § 1801(e) (definition of foreign intelligence information). Thus, not only does the government overstate the necessity and urgency of § 702 collections by relying on only part of the information it is authorized to search and seize without a warrant, it also entirely ignores the reality that judicial oversight can

be adapted to meet any legitimate needs in terms of "fast-moving threats," as has been done in other parts of FISA. In short, the government presents a false dichotomy by suggesting a zero-sum choice must be made between individualized judicial oversight and national security.

Individualized judicial review before the government retains and accesses the content of Americans' electronic communications is not only required by the Constitution, but also by the statute. Section 702 explicitly uses "foreign intelligence information," which is defined in 50 U.S.C. § 1801(e). 50 U.S.C. §§ 1881a(a) & (g)(2)(A)(v). Section 1801(e) incorporates separate standards for foreigners and United States persons: for communications of foreigners, the information may be seized if it "relates to" subjects including "the conduct of the foreign affairs of the United States;" when communications are "concerning a United States person," instead of "relates to," the information must be "necessary to" the conduct of foreign affairs, among other subjects. 50 U.S.C. § 1801(e)(2). Thus, the statute on its face requires a separate assessment for collected communications that are "concerning a United States person." Any government complaint that separate assessment is impracticable should be made to Congress, where the requirement was imposed, and not to this Court.

Further, if the government is complaining that the volume of American communications seized makes individual assessment impracticable, then this is evidence that the government's mass dragnet of communications far exceeds what the statute authorized. If the government is complaining about the interposition of a decision-node within its collections, the statute contemplated such a step as necessary to protect Americans from overbroad intrusions under vague standards. To construe the statute to avoid serious constitutional problems, the determination that the government is authorized to collect, database, and examine the content of Americans' electronic

communications should be made by a judicial officer in accordance with traditional FISA and Fourth Amendment standards.

e. Concerns About Meaningful Protection For Americans' Electronic Communications Are Not "Considerably Diminished" In The Context Of Collection Of Foreign Intelligence.

The government suggests that the Fourth Amendment's warrant requirement is not as important in the context of foreign intelligence because the Executive Branch has "superior expertise" with respect to that subject matter, while the constitutional interests at stake relate to "interpos[ing] a judicial officer between the zealous police officer ferreting out crime and the subject of the search." CR 509 at 40. This argument should be rejected for several reasons.

The Fourth Amendment protects American citizens' privacy rights without regard to which government actors are involved. Privacy rights are infringed in exactly the same way regardless of whether the intruding individual is a zealous police officer or a zealous NSA analyst. Nor is there any reason to believe that Executive actions with respect to foreign intelligence surveillance will somehow result in fewer privacy abuses than would occur with ordinary law enforcement officers. To the contrary, history has proven such an assumption false, which is the fundamental reason that FISA was originally enacted. *See* S. Rep. No. 95-604(1) (FISA meant to curb "the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it"); *see also In re National Security Telecommunications Records Litigation*, 564 F. Supp. 2d 1109, 1117 (N.D. Cal. 2008) (FISA's repeal of 18 U.S.C. § 2511(3) eliminated "any congressional recognition or suggestion of inherent Presidential power with respect to [foreign intelligence] electronic surveillance.") (quoting S. Rep. 95-701, 72).

Moreover, the national debate occurring now in the aftermath of the Snowden disclosures is almost entirely based on purported Executive Branch excesses with respect to surveillance. A recent book published by one of the journalists involved in the Snowden affair recounts a 2008 statement by then-NSA director Keith Alexander to the effect: "Why can't we collect all the signals, all the time?" David Cole, "*No Place to Hide" by Glenn Greenwald, on the NSA's sweeping efforts to "Know it All*," Wash. Post, May 12, 2014. Mr. Greenwald's book also documented a 2011 meeting in which the "NSA described its 'collection posture' as 'Collect it All,' 'Process it All,' 'Exploit it All,' 'Partner it All,' 'Sniff it All,' and ultimately, 'Know it All.'" *Id*. Given the recent giant strides toward a surveillance state, the need for judicial oversight of Executive surveillance activity of American citizens is not "considerably diminished" merely because the context may involve foreign affairs. CR 509 at 40.

Because the § 702 authorizes the unchecked mass collection and retention of Americans' private electronic communications based on nebulous "foreign intelligence" grounds, the government's attempt to invoke an exception to the Warrant requirements should be rejected.

3. The Government's Acquisition, Retention, And Accessing Of Americans' Electronic Communications Violate Core Privacy Interests Protected By The Warrant Clause And Constitute Unreasonable Searches And Seizures.

The Court need not reach the government's reasonableness argument because any foreign intelligence exception is far narrower than the foreign affairs surveillance in the present case. *See Directives*, 551 F.3d at 1012 ("we hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists 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.") (emphasis added). In advocating for a "general reasonableness test," the government abandons any reference to Warrant Clause norms and undertakes balancing based on misconstruction of the interests at stake. CR 509 at 41-44. Contrary to this approach, the threshold question regarding foreign intelligence gathering is whether a warrant is required. *Zweibon*, 516 F.2d at 633.

Even on reasonableness, although referencing *Directives* repeatedly, the government makes no mention of the court's unequivocal use of the Warrant Clause as the key metric in determining reasonableness: "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." *Directives*, 551 F.3d at 1013. Under that standard, the vast distance between the six components of the Warrant Clause and the dragnet acquisition, retention and accessing of American communications under the FAA demonstrates the unreasonableness of the § 702 programs. CR 503 at 17-28. In the absence of any meaningful analogies to Warrant Clause protections, the government relies on inapt references to DNA and drug screening, always omitting the limitations of those cases as exceptions to warrant requirements. For example, the DNA swab of arrestees involved a "negligible" intrusion, *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013), while this case involves listening to and reading Americans' private – and sometimes intimate – electronic communications. The DNA cases involve no discretion exercised by officers: the officers simply need "a safe and accurate way to process and identify the persons and possessions they must take into custody." *Id*. Similarly, the Court has approved probation searches based on the significantly diminished expectation of privacy, prior notice, and the need for probation officers to provide supervision in the

community. *Samson v. California*, 547 U.S. 843 (2006); *United States v. Knights*, 534 U.S. 112 (2001).[7]

In contrast, under the FAA, there are virtually no limits: the persons who might be targeted are broadly defined; the purposes of surveillance include anything related to foreign policy, and the intelligence agencies, once in possession of communications, claim they have completely unrestricted authority to do anything they want with Americans' private communications. The cases relied on by the Government simply provide no useful analogy to the mass acquisition, retention, and accessing of Americans' electronic communications under the FAA.

a. The Government Interest At Stake Is Too Broadly Defined To Justify The Mass Acquisition, Retention, And Accessing Of Americans' Electronic Communications.

The government's claim of a national security interest of the highest magnitude must be closely scrutinized. As an initial matter, the government fails to acknowledge the difference recognized in *Sealed Cases* between national security "protective" and "counterintelligence" information, which under § 1801(e)(1) involves terrorist attacks, sabotage, and clandestine activities of foreign spies, and the relatively innocuous "affirmative" or "positive" material that can inform the conduct of foreign affairs under § 1801(e)(2). 310 F.3d at 723 n.9. On its face, § 702 encompasses both purposes under § 1801(e). Thus, despite the government's repeated invocations of "threats" to national security, § 702 authorizes warrantless surveillance of Americans' communications for far more mundane purposes. Although the government's description of the

[7] The individualized temporary detention needed to preserve a scene while a search warrant is obtained is even more remote from the issues in this case. *See Illinois v. McArthur*, 531 U.S. 326 (2001).

program is mostly redacted, the Court should find the acquisitions authorized are extremely overbroad and indiscriminate in light of the absence of any statutory limitation focusing narrowly on national security, as opposed to generally useful and relevant "foreign affairs" information. While even a proper invocation of national security would not provide the government with a blank check for warrantless intrusions, *Keith*, 407 U.S. at 320, the government interest in this case is far more general and lacking in exigency, thereby detracting from the reasonableness of the individual privacy intrusion with no judicial review or supervision.

The government's reliance on the supposed involvement of the § 702 program in 54 counterterrorism investigations is troubling. CR 509 at 46-47. When Senator Leahy challenged that the figure during a Senate hearing, the Director of the NSA dropped considerably the number of relevant cases:

> SEN. LEAHY: Let's go into that discussion, because both of you have raised concerns that the media reports about the government surveillance programs have been incomplete, inaccurate, misleading or some combination of that. But I'm worried that we're still getting inaccurate and incomplete statements from the administration.
>
> For example, we have heard over and over again the assertion that 54 terrorist plots were thwarted by the use of Section 215 and/or Section 702 authorities. That's plainly wrong, but we still get it in letters to members of Congress; we get it in statements. These weren't all plots, and they weren't all thwarted. The American people are getting left with an inaccurate impression of the effectiveness of NSA programs.
>
> Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and out of the 54, only 13 had some nexus to the U.S. Would you agree with that, yes or no?
>
> DIR. ALEXANDER: Yes.

Continued Oversight of FISA Surveillance Programs: Hearing Before the S. Comm. on the Judiciary, 113th Cong. at 43:00 (Oct. 2, 2013) (statement of Keith B. Alexander, Director, NSA).[8]

Director Alexander then qualified that, of the thirteen, two were involved with § 215, not § 702. *Id*.; *see generally First Unitarian Church of Los Angeles v. NSA*, No. 3:13-cv-03287-JSW, Brief of Amici Curiae Senator Ron Wyden, Senator Mark Udall & Senator Martin Heinrich in Support of Plaintiffs, filed Nov. 18, 2013. Eleven cases where there was unspecified involvement of § 702 falls far short of counter-balancing the massive loss of privacy of millions of Americans. The Court should not rely on the bald statements of the government, which maintains a monopoly on information, in the absence of the adversary proceedings necessary to test the government's claims. The government, even as it fails to differentiate cases involving American electronic communications, which are the only communications at issue, provides a footnote with [CLASSIFIED MATERIAL REDACTED], once again emphasizing the need for adversary participation of the defense to arrive at a fair and reasonable dispostion. CR 509 at 47 n.31.

b. Americans Have A Reasonable Expectation Of Privacy In Their Electronic Communications, Regardless Of Routing Or Destination.

Ignoring the basic principle that the Fourth Amendment "protects people, not places," *Katz v. United States*, 389 U.S. 347, 351 (1967), the government argues that "U.S. persons have limited expectations of privacy in their electronic communications with non-U.S. persons outside the United States." (CR 509 at 47). This is not the law, and the Court should not condone the massive violation

[8] Available at http://cs.pn/18jdL2b.

of privacy rights that would ensue if this principle were accepted.[9] When a person in the United States pens a letter, or writes an email, or communicates on a telephone, that person has a reasonable expectation of privacy in the communication. *Keith*, 407 U.S. at 313 ("[*Katz*] implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."); *Alderman v. United States*, 394 U.S. 165, 177 (1969) (phone calls); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (emails). The Fourth Amendment's protection extends not just to domestic communications but to international ones as well. *See*, *e.g.*, *United States v. Ramsey*, 431 U.S. 606, 616–20 (1977). In the absence of a warrant or judicially recognized exception to the warrant requirement, the government cannot search that communication in the United States without violating the Fourth Amendment. The government's arguments to the contrary should be dismissed.

The government relies on cases establishing that no Fourth Amendment protection exists for information voluntarily disclosed to others (*e.g., United States v. Miller*, 425 U.S. 435, 443 (1976), *Couch v. United States*, 409 U.S. 322, 335 (1973), *Hoffa v. United States*, 385 U.S. 293, 302 (1966)), but then attempts to extend this principle to instances where the disclosure was not voluntary: "the same principle applies whether the recipient intentionally makes the information public or stores it in a place subject to government search." CR 509 at 48. That argument is the equivalent of saying

---

[9] Although in the brief in this case the government argues that Americans' privacy interests are "significantly diminished" when they write to people overseas, in its pleading filed shortly afterwards in a similar case in Colorado, the government extended its argument still further, arguing that such privacy rights "are significantly diminished, *if not completely eliminated*," when directed to people overseas. *See United States v. Muhtorov*, 12-CR-33-JLK, CR 559 at 35 (D. Col. filed May 9, 2014) (emphasis added). This extension indicates the sweep of the government argument and demonstrates that once the argument about "diminished" rights is accepted, there is no boundary between diminished and no privacy rights at all.

that a person has a privacy interest in a letter inside one's home, but not after it is handed over to the letter carrier, where it could be "subject to government search." The Supreme Court has unequivocally rejected that argument. *See United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."). The government cannot snatch a communication as it is being transmitted, then store and later access its contents, without Fourth Amendment consequences.

Moreover, the fact that a communication has been received and held by the recipient does not authorize the government to seize the communication without the consent of the recipient. The government argues that a "sender's expectation of privacy ordinarily terminates upon delivery," (CR 509 at 48), but fails to complete the thought: and then what? The government can then, therefore, go into the home of the recipient and take the letter that has been delivered? When spelled out, the idea is preposterous, but this is precisely what the government suggests it can do with emails, when it attempts in a footnote to distinguish *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), arguing that the Fourth Amendment does not apply when the government obtains emails from someone else's account. CR 509 at 48 n.32.

Because the searches conducted under § 702 occur within the United States and not at the border, the government recognizes it cannot rely on the border search exception to justify its warrantless incursions into data lines and email accounts (CR 509 at 50) ("the government does not contend that the Section 702 collection here was per se reasonable under the border search doctrine"). The border search doctrine is a narrowly tailored exception to the Fourth Amendment grounded in the "right of the sovereign to control . . . who and what may enter the country." *Ramsey*,

431 U.S. at 620; *see also id.* at 619 ("Border searches . . . have been considered to be 'reasonable' by the single fact that the person or item in question has entered our country from outside."); *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (recognizing exception for "routine searches of the persons and effects of entrants").[10] The government's suggestion that "principles" from the border search context are relevant to the analysis here attempts to extend the exception beyond its limits. Indeed, because electronic and telephonic communications routinely cross international borders even when both parties are within the United States, use of the border search exception for electronic searches would allow the government to search every domestic email and phone call without limit.[11]

c. The § 702 Programs' Procedures For Retention And Accessing – Which Must Be Considered In The Fourth Amendment Analysis – Are Unreasonable Because They Provide Inadequate Protection For The Privacy Of Individual American Citizens.

Another argument that runs throughout the government's response is that its minimization and other procedures provide adequate protection to what it calls incidentally seized communications of United States persons. CR 509 at 9, 15, 17-23, 25-27, 30, 43-45, 51-55, 57-61, 62, 64-68, 73-76,

[10] The government cites *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), for the proposition that the border search exception applies to "persons and property entering or *exiting* the country" (CR 509 at 49) (emphasis added), but that citation does not support the search of items exiting the country, and the Supreme Court justifies the exception based only on controlling entry of items or people into the United States. The Ninth Circuit, however, has extended the border search doctrine to include exits as well as entry into the country. *See United States v. Seljan*, 497 F.3d 1035, 1040 (9th Cir. 2007); *United States. v. Des Jardins*, 747 F.2d 499, 504 (9th Cir. 1984), *vacated in part*, 772 F.2d 578 (9th Cir. 1985).

[11] The government acknowledges that "Today, a single communication can transit the world even if the two people communicating are only located a few miles apart." CR 509 at 19.

83. Its argument about these procedures ignores both the facts known regarding its procedures and the law. As stated in *[Case Name Redacted]*,

> The [FISA] Court of Review and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information.

2011 WL 10945618, at *27. At the outset then, the government is simply ignoring the very cases on which it relies when it claims that the Fourth Amendment has no application to what it does with information once it has seized it. CR 509 at 55-57.

The government's analysis also fails to recognize what the FISC and FISA Court of Review have held regarding what is at issue in addressing FAA surveillance. Under the FAA, the ex parte courts review the legality of a search and seizure "program" as a whole. *Id*. This Court must, therefore, analyze the issues before it in this case not in isolation but as the fruit of a "program" that fails to pass constitutional muster.

The government's analysis also repeatedly uses straw man arguments. CR 509 at 27, 38. The defense is not seeking to have this Court find that the government may not use § 702 to seize communications of foreigners overseas or that warrants are required for all such activity. The arguments are far more limited: because use of § 702 results in seizure of a significant number of communications of United States persons, the program must be structured to provide protections to those communications – and it does not.

With respect to the constitutionality of the statute, the government's arguments in support of the FAA program include the limitation in § 702 to acquisition of information with a "significant purpose" to "obtain foreign intelligence information." CR 509 at 37. It fails to recognize, however, that the "foreign intelligence" limitation only applies to the "acquisition" of information and not to

later querying. In arguing in its response that the Fourth Amendment has no application once a communication has been seized (CR 509 at 56), the government is necessarily arguing that none of the statutory limitations on acquisition on which it relies have any bearing on or provide any protection from its retention, querying, uses, and disseminations.

The defense is handicapped in addressing the deficiencies in the minimization and other procedures because the government has not disclosed those at issue here. But the procedures are evidently inadequate because the statute itself is circular, allowing the government to do, essentially, whatever it claims it needs. This is because the last clause of 50 U.S.C. § 1801(h) requires limitations only to the extent they are "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." The limitations, therefore, eviscerate the whole. From what is known about the limitations in place, the primary, or only, limitations on "retention" are the multi-year periods of varying length set by various government agencies. Allowing retention of communications of United States persons for two or five years provides no meaningful privacy protection, especially when the contents of Americans' communications can be repeatedly accessed without limitation throughout that time.

The decision in *[Case Name Redacted]* includes a discussion of the evolution of the NSA minimization procedures with respect to querying of its database after the acquisition of communications. 2011 WL 10945618, at *7. That discussion raises several issues. First, it includes the fact that the NSA minimization procedures have evolved over the years and, at some point, possibly during the time when information was gathered against Mr. Mohamud, the procedures "effectively impose[d] a wholesale ban on queries using United States-Person identifiers." *Id*.

Second, the fact that the procedures approved by the FISC have changed to permit such queries subject to certain procedures and approvals further undermines the government's argument that the Fourth Amendment is irrelevant to subsequent queries. It also underscores the need for full adversarial fact development and argument about the constitutionality of such queries. Some members of the FISC, and potentially either the Bush or Obama administrations, have apparently understood that strong protections are required with respect to the use of United States person communications obtained through § 702 activity.

The cases cited by the government in support of its argument that subsequent searches are not "separate searches" and do not involve any further invasions of privacy are all distinguishable. In *United States v. Diaz-Castenada*, 494 F.3d 1146 (9th Cir. 2007), the court considered publicly visible information (license plate numbers) in a highly regulated activity. Other cases involved DNA information collected from criminal offenders. *Boroian v. Mueller*, 616 F.3d 60 (1st Cir. 2010); *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir. 2006). Such people have had the benefit of full judicial review of their conduct before their DNA can be placed in a database.

The government's discussion of *Jabara v. Webster*, 691 F.2d 272 (6th Cir. 1982), is particularly incomplete. The government correctly notes that Mr. Jabara did not contest the interception of his communications. Here, the defense does contest the initial interception as occurring under a "program" that is defective because it does not contain sufficient protection for United States persons, nor did *Jabara* involve a claim that there was a subsequent search conducted by the government that led to the transmission of the seized communication from the NSA to the FBI. This case does.

In *Jabara*, the court recognized the critical distinction that the government repeatedly ignores in its response between seizure and search: "The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents." 691 F.2d at 278 (quoting *Walter v. United States*, 447 U.S. 649, 654 (1980)). Subsequent searches for information, such as those at issue in *Jabara* and here, require separate grants of authority under the Fourth Amendment.

Ultimately, there are no real protections for Americans' communications under § 702 at any stage of the process, whether targeting, retention, or later access. The government's interests are too broadly defined to allow compromise of the privacy of Americans, who retain their full expectations of privacy in their electronic communications. Therefore, even if a warrant were not required, § 702 is unreasonable under the Fourth Amendment.

B. Section 702 Blurs The Constitutionally Required Separation Of Powers By Providing Article III Judges The Role Of Designing Programs, Rather Than Ruling On Individual Applications To Authorize Surveillance, And By Delegating To Article III Judges Legislative And Executive Functions Far Afield From The Judicial Role Of Deciding Cases And Controversies.

The government's response fails to account for the fundamental difference between ex parte review of an application for authorization to conduct a specific search, and the general programmatic authorization that judges undertake under § 702. CR 509 at 65-69. In close cooperation with government agents and prosecutors, judges help design programs that result in the search and seizure of the electronic communications of unspecified United States citizens. The § 702 program involves judicial officers in the non-judicial role of designing programs, rather than determining whether, under legislatively or executively-established standards, a particular search and seizure is authorized by law.

The Supreme Court in *Booker v. United States*, 525 U.S. 738, 755 (2005), reaffirmed the separation of powers limitations that should apply here: "[W]e have not hesitated to strike down provisions of law that either accrete to a single Branch powers more appropriately diffused among separate Branches or that undermine the authority and independence of another coordinate Branch" (citing *Mistretta v. United States*, 488 U.S. 361, 382 (1989)). Where the statute coopts judges to design Executive programs, while the judges make no determinations based on individualized suspicion regarding specific subjects of Executive interest, the Court should strike down the provisions as both exceeding the proper functions of the separate branch of government and undermining the independence of the Judiciary. *See Mistretta*, 488 U.S. at 380 ("This Court has consistently given voice to, and has reaffirmed, the central judgment of the Framers of the Constitution that, within our political scheme, the separation of governmental powers into three coordinate Branches is essential to the preservation of liberty.").

While it is not required that the three Branches be entirely separate and distinct, *Mistretta*, 488 U.S. at 380, the outer limit of appropriate congressional delegation to the Judiciary is expressed in Article III of the Constitution, under which "[t]he judicial power of the United States is limited to 'Cases' and 'Controversies.'" *Mistretta*, 488 U.S. at 385 (citing *Muskrat v. United States*, 219 U.S. 346, 356 (1911)). As the Court in *Mistretta* explained: "[t]hese doctrines help to ensure the independence of the Judicial Branch by precluding debilitating entanglements between the Judiciary and the two political Branches, and prevent the Judiciary from encroaching into areas reserved for the other Branches by extending judicial power to matters beyond those disputes 'traditionally thought to be capable of resolution through the judicial process.'" *Mistretta*, 488 U.S. at 385 (quoting *Flast v. Cohen*, 392 U.S. 83, 97 (1968)); *see also Clinton v. City of New York*, 524 U.S.

417, 440-47 (1998) (line item veto violated separation of powers by conferring upon the President the power to amend statutes).[12]

The government's repeated citations to cases upholding FISA ex parte decisions regarding the issuance of surveillance orders in individual cases are irrelevant. CR 509 at 65-66. As *Keith* held, Congress could design warrant analogues to permit surveillance under appropriate legal standards. 407 U.S. at 322-23. The FAA involves a quantum leap away from individualized judicial review to generalized programmatic design. As seen in the *[Case Name Redacted]* opinion, the judge's review and collaboration with Executive Branch attorneys involves the general design of administrative programs, with no judicial review of any individual acquisition, retention, and accessing of the Americans' communications. 2011 WL 10945618, at *1-3; *see Morrison*, 487 U.S. at 677 ("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.'") (citations omitted).[13]

In addition to the abandonment of the judicial role, the participation of judicial officers in the design of the collection program violates the non-delegation doctrine because the statute fails to

---

[12] Although the FISA Review Court found no problem with the FISC's secret and non-adversarial proceedings regarding specific surveillance orders, "administrative guidance" outside the normal judicial role, here under FAA programmatic surveillance, raises precisely the issues of a program that may be "a bureaucratic success story, but it would have serious constitutional ramifications." *Sealed Cases*, 310 F.3d at 732 (quoting *Morrison v. Olson*, 487 U.S. 654, 684 (1988)).

[13] Contrary to the government's suggestion (CR 509 at 65 n.1), the programmatic surveillance authorized in § 702 bears no resemblance to the rules of procedure that Congress "expressly has authorized" for the Judiciary to promulgate in order to conduct its own business. *Mistretta*, 488 U.S. at 388.

provide clearly delineated policies that specify the boundaries of the delegated authority. *Mistretta*, 488 U.S. at 372-73. The design of the programmatic surveillance program includes the unguided instruction to design a program not to violate the Fourth Amendment. 50 U.S.C. § 1881a(b)(5). Given the Fourth Amendment's reasonableness requirement, and the possibility that the least intrusive search does not determine the limits of reasonableness (*Quon*, 130 S. Ct. at 2632), Article III judges are being assigned a legislative and executive function that also compromises the judicial neutrality necessary to adjudicate whether a search authorized by the judges' program violates the Fourth Amendment.

In the end, the government relies on analogy to administrative searches approved in *Camara v. Municipal Court*, 387 U.S. 523 (1967). CR 509 at 68-69. The dicta in *Camara* (the case itself did not involve an administrative warrant) provides little assistance to the government.[14] There is not the slightest suggestion that judges could appropriately participate in designing the administrative guidelines for housing inspector searches. Similarly, as former FISC Judge Robertson told the Oversight Board, the design of search and seizure programs under § 702 is better viewed as an administrative task of the Executive branch that is outside the judicial bailiwick. PCLOB hearing at 36 (July 9, 2013). As the government observes, "warrant or wiretap applications for law enforcement purposes typically involve a more fact-specific form of review." CR 509 at 69.

---

[14] In addition to providing no basis for judicial participation in promulgating administrative rules, the case respected the role of warrants in individual cases: Because most citizens allow inspections of their property without a warrant, "as a practical matter and in light of the Fourth Amendment's requirement that a warrant specify the property to be searched, it seems likely that warrants should normally be sought only after entry is refused unless there has been a citizen complaint or there is other satisfactory reason for securing immediate entry." *Camara*, 387 U.S. at 539-40.

Section 702 improperly incorporates the Judiciary into the Executive function of designing search and seizure programs, delegates Legislative functions to the Judiciary without delineating the scope of the programs with intelligible and limiting guidelines, and compromises the Judiciary's neutrality in judging the application of the programs to a particular individual citizen. It is, therefore, unconstitutional, facially and as applied.

C. Section 702 Violates The First Amendment Because Its Overbreadth And Vagueness Chills Exercise Of Speech, Press, Religious, And Associational Rights.

Courts have repeatedly recognized that the government's investigatory and surveillance activities can infringe on rights protected by the First Amendment—and that the First Amendment has force independent of the Fourth Amendment. *See*, *e.g.*, *Stanford v. Texas*, 379 U.S. 476, 484-85 (1965) ("The bill of rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 547(1963) (underscoring the substantial "deterrent and 'chilling' effect on the free exercise of constitutionally enshrined rights of free speech, expression, and association" resulting from government investigation and compelled disclosure of political associations); *see also Perry v. Schwarzenegger*, 591 F.3d 1126, 1136 (9th Cir. 2009) ("Compelled disclosures concerning protected First Amendment political associations have a profound chilling effect on the exercise of political rights."). The government's massive surveillance of communications under § 702 burdens First Amendment rights by exposing Americans' associational contacts and political thoughts and writings to government monitoring and scrutiny.

In its breadth and scope, the FAA program of acquiring, databasing and querying the emails and other communications of Americans far exceeds the demands for basic membership rolls that

the Supreme Court assessed in *NAACP v. Alabama,* 357 U.S. 449 (1958), and its progeny. *See Gibson*, *supra*; *Bates v. City of Little Rock*, 361 U.S. 516 (1960). A corollary of this direct intrusion on Americans' communications is the chill it imposes on all who would ordinarily communicate by phone and email. Generalized surveillance on this scale "chills associational and expressive freedoms." *See Jones v. United States*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). This harm amounts to substantial and discrete burdens on First Amendment rights.

The government errs in urging the Court to reject the defense's First Amendment claim on technical grounds. First, the government argues that there is no judicially-created exclusionary rule to remedy violations of the First Amendment. CR 509 at 69-70 (citing cases noting that suppression of evidence is a Fourth Amendment claim). That point is irrelevant, however, because Congress has provided a *statutory* remedy of suppression for "unlawful" surveillance, which undeniably applies to this case. 50 U.S.C. § 1806(e) and (g) (authorizing motion to suppress evidence obtained through unlawful surveillance and providing remedy of suppression). Actions that are unconstitutional – under the First, the Fourth, or any Amendment – are "unlawful." *See, e.g., FCC v. Fox Television Stations, Inc*., 556 U.S. 502, 516 (2009) (noting statute provides remedy for "unlawful" action "which of course includes unconstitutional action"). The cases cited by the government concerning

the judicially-created exclusionary rule are a red herring and should not govern the Court's decision.[15]

Second, although the government is correct that the plantiffs in *Clapper* were not able to establish standing to bring a constitutional challenge to the FAA because their "fear of surveillance" was "too speculative" (CR 509 at 71), there is no dispute here that Mr. Mohamud has standing, as an aggrieved party, because his communications were in fact seized. The government's statutory notice acknowledges this fact. CR 509 at 2. As an aggrieved party, Mr. Mohamud can bring a facial challenge to the statute on behalf of other harmed persons. *Acosta v. City of Costa Mesa*, 718 F.3d 800, 811 (9th Cir. 2013) (finding statute overbroad and noting facial challenge on First Amendment grounds can be made when "there [is] a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court.").

Third, the government's statement that the defense cannot show "that the government has conducted such collection with any purpose to suppress expressive or associative activity" (CR 509 at 71) is not relevant, because the Supreme Court has established that a First Amendment injury does not depend on an intent to curtail speech. *See, e.g., Elrod v. Burns,* 427 U.S. 347, 362 (1976) (noting that First Amendment injury can occur through the "unintended but inevitable result of the government's conduct").

Finally, case law does not support the government's suggestion that the First Amendment claim need not be addressed if the government complied with vague Fourth Amendment "standards"

---

[15] The government cites *United States v. Mayer*, 503 F.3d 740, 747 (9th Cir. 2007), but that case involves a defendant's efforts to suppress evidence obtained by an undercover informant's infiltration of a meeting in the absence of a statutory basis for suppression of evidence.

(CR 509 at 70-71). Instead, the courts have applied the Fourth Amendment's "warrant requirements with particular exactitude when First Amendment interests would be endangered by the search." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (relying specifically on the warrant requirements of specificity and probable cause); *Armstrong v. Asselin*, 734 F.3d 984, 993-94 (9th Cir. 2013) ("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"). In some cases, the precise safeguards required by the Fourth Amendment may satisfy the First Amendment as well. *Zurcher*, 436 U.S. at 565. In this case, given the government's predominant argument that the Fourth Amendment's warrant requirements do not apply to § 702 searches at all (CR 509 at 27-40), the government's reliance on cases applying precisely those requirements of probable cause and particularity is ironic at best. The Court should assess the First Amendment claim on its own merits, without subordinating it to Fourth Amendment analysis.

Section 702 violates the First Amendment because it is both overbroad and vague. CR 503 at 37-38. The overbreadth and vagueness doctrines are well-established methods of challenging imprecise laws:

> First, the overbreadth doctrine permits the facial invalidation of laws that inhibit the exercise of First Amendment rights if the impermissible applications of the law are substantial when "judged in relation to the statute's plainly legitimate sweep." . . . Second, even if an enactment does not reach a substantial amount of constitutionally protected conduct, it may be impermissibly vague because it fails to establish standards for the police and public that are sufficient to guard against the arbitrary deprivation of liberty interests.

City of Chicago v. Morales, 527 U.S. 41, 52 (1999) (citations omitted). Under the overbreadth doctrine, a statute may be facially invalid if the threat of its enforcement "deters people from

engaging in constitutionally protected speech, inhibiting the free exchange of ideas." *United States v. Williams*, 553 U.S. 285, 292 (2008).

The first step in the analysis is to construe the statute, because "it is impossible to determine whether a statute reaches too far without first knowing what the statute covers." *Id*. In this case, § 702, as construed by the government, permits surveillance of all communications to foreign "persons" (which includes individuals, entities, groups or foreign powers) for information involving "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1881a(a) and 1801(e)(2)(B).[16] The communications "to" foreign persons may be communications by Americans from within the United States.

The second step is to determine whether the statute, as construed, covers "a substantial amount of protected expressive activity." *Id.* at 297. The sweep of § 702's surveillance of protected First Amendment activity is enormous. Under the language of the surveillance the government could capture, for example, an American's email to a grandparent overseas that is "about" Guantanamo, or "about" Al Queda, even though neither the sender nor recipient has any relevance to a foreign

---

[16] The relevant text of the FAA, 50 U.S.C. § 1881a(a) states:

> 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.

The definitions of "persons" and "foreign intelligence information" are in 50 U.S.C. § 1801(e) and (m).

intelligence purpose.[17] Moreover, capturing communications about the "conduct of foreign affairs" is political speech, deserving of the highest protection. The government has not disclosed exactly how many hundreds of thousands of such emails have been "incidentally" obtained under § 702, but the volume is massive. Because § 702 permits the government to gather up a substantial amount of communication "beyond the statute's plainly legitimate sweep," and then review it, and because this governmental intrusion into private communications chills protected speech, § 702 is overbroad and violates the First Amendment.

The vagueness of the statute also chills protected associational and communicative activity. By the plain words of the statute, one might not recognize that Americans' communications are being "incidentally" gathered up under § 702. And yet, as the press reports on leaks and government admissions about the program have become more widespread, Americans have changed their on-line behavior or self-censored their communications (CR 503 at 38). The shadow of surveillance may be as oppressive as the surveillance itself:

> The First and Fourteenth Amendment rights of free speech and free association are fundamental and highly prized, and 'need breathing space to survive.' . . . 'Freedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference.'"

Gibson, 372 U.S. at 544. In this case, the Court should find § 702 unconstitutional because, through its overbreadth and vagueness, it compromises and diminishes cherished rights in violation of the

[17] The government has publicly claimed it does not use such broad terms in its "targeting" procedures. While the defense is not in a position to assess that claim, it is clear that nothing in the text of § 702 prevents such targeting. Further, there are certainly technological means to effect the same surveillance without using broad terms like the name of a country (*e.g.*, target country emails ".ru" instead of "Russia").

First Amendment. The use of this unconstitutional statute in this case was "unlawful," and under 50 U.S.C. § 1806(e), the evidence thereby derived must be suppressed.

D. Both FISA And The Constitution Require Suppression Of Any Unlawfully Obtained Or Derived Evidence.

The government claims that, assuming it acted unlawfully in conducting the warrantless electronic surveillance, the Court should deny the motion to suppress based on *United States v. Leon*, 468 U.S. 897 (1984). On the contrary, the Court should grant the motion to suppress, both under the statutory exclusionary rule under 50 U.S.C. § 1806(g) and the constitutionally-based exclusionary rule under *Wong Sun v. United States*, 371 U.S. 471 (1963).

If the surveillance was "not lawfully acquired or conducted," the evidence obtained or derived from" the electronic surveillance "shall" be suppressed under § 1806(g). If the statute is unconstitutional, the electronic surveillance was neither lawfully acquired nor conducted. *See ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) ("The Constitution is law" as FISA uses that term); *see* H. Rep. No. 95-1283 at 92-93 (1978) (in reviewing a motion to suppress FISA evidence, the trial court "is also free to review the constitutionality of the law itself."). As with Title III wiretaps, violation of the statute as well as constitutional violations result in suppression under the fruit of the poisonous tree doctrine. *United States v. Giordano*, 416 U.S. 505, 524-32 (1974). As with Title III, the language and legislative history of the FISA statutory exclusionary rule – which preceded the existence of *Leon* – does not include a good faith exception. *See United States v. Rice*, 478 F.3d 704, 711-14 (6th Cir. 2007) ("The language and legislative history of Title III strongly militate against engrafting the good-faith exception into Title III warrants."). The statutory

exclusionary rule applies without qualification and must result in the suppression of all information obtained through the warrantless surveillance and all derivative actions and evidence.

On the non-statutory exclusionary rule, the government's reference to *United States v. Ning Wen* and other similar cases involve the distinguishable situation where officers relied on an individualized FISA or other judicial order. 477 F.3d 896, 897-88 (7th Cir. 2007). There is no reasonable analogy to *Leon* under the FAA where there was no individualized judicial review that authorized a specific surveillance, especially given the unconventional mixing of judicial and executive functions in designing the programmatic surveillance. In any event, the court in *Ning Wen* found the surveillance to be authorized, so the reference to good faith was dicta. Given the Solicitor General's arguments in *Clapper* about the effectiveness of § 1806(c) notice in obtaining the constitutional review, which was thwarted in that case based on standing, the government's claim that such review would be fruitless should be rejected. The government knew from the day of enactment in 2008 the parameters of the constitutional objections to the statute due to the immediate initiation of litigation in *Clapper*. The Court should reject any claim based on a good faith exception that would render a defendant's constitutional challenge futile.

E. The Court Should Grant Discovery Because The Factual And Legal Complexity Of These Motions Require Adversary Proceedings Under FISA And The Due Process Clause.

There is obvious unfairness in the government's position that, on one hand, the defense can only bring an as applied challenge, while on the other hand, the defense should not be permitted to learn the facts of how the statute was applied. CR 509 at 80-87. As outlined in the previous discovery pleadings (CR 489, 493, 496, 498), the Court should grant full adversarial participation by the defense. The statutory context and the legislative purpose, as supported by the legislative

history, demonstrate that "necessary" within the meaning of 50 U.S.C. § 1806(f) means the Court would be assisted by adversary proceedings, not that they are essential.

"The term 'necessary' is a chameleon-like word whose meaning . . . may be influenced by its context . . . [It] is not language of plain meaning." *Cellco Partnership v. FCC*, 357 F.3d 88, 96-97 (D.C. Cir. 2004). Rather than look to statutory context and purpose, the government claims the defense must be excluded if the Court is "able" to assess the legality of the collection, and that disclosure has never and should never happen. CR 509 at 81-82. The Court should reasonably construe "necessary" to include the present circumstances, which easily fit within the conditions for adversary proceedings anticipated by the legislative history.

1. Section 1806(f)'s Context And Legislative Purpose Demonstrate That The Government Misreads The Statute As Creating A Rule Of Nondisclosure.

Section 1806(f) authorizes the Court to disclose materials relating to surveillance to the defense when "necessary" to make an accurate determination of the legality of the surveillance. The government misconstrues "necessary" as if it means "essential." Courts have frequently interpreted the word "necessary" "to mean less than absolutely essential, and have explicitly found that a measure may be 'necessary' even though acceptable alternatives have not been exhausted." *CT&IA v. FCC*, 330 F.3d 502, 510 (D.C. Cir. 2003) (quotation omitted); *see McCulloch v. Maryland*, 17 U.S. (4 Wheat) 316, 413-16 (1819) ("necessary" in the Necessary and Proper Clause does not mean "absolutely necessary"). In *Commissioner v. Tellier*, the Court found that the word "necessary" in the phrase "ordinary and necessary [business] expenses" imposes "only the minimal requirement that the expense be appropriate and helpful for the development of the taxpayer's business." 383 U.S. 687, 689 (1966) (quotations and brackets omitted). In context, the word "necessary" in § 1806(f)

should be interpreted as closer to "helpful" and "appropriate" than "absolutely necessary" in light of statutory context and legislative purpose.

The word "necessary" has "always been recognized as a word to be harmonized from context." *Armour & Co. v. Wantock*, 323 U.S. 126, 130 (1944). In context, "necessary" has frequently been determined to mean appropriate or helpful rather than essential. *See*, *e.g.*, *Snider v. United States*, 468 F.3d 500, 513 (8th Cir. 2006) (in tax code, "'appropriate or helpful' meaning of 'necessary' is the only practical interpretation in this context"); *Prometheus Radio Project v. FCC*, 373 F.3d 372, 393-94 (3d Cir.2004) (interpreting "necessary" in the Telecommunications Act of 1996 to mean "'convenient,' 'useful,' or 'helpful,' not 'essential' or 'indispensable'"); *FTC v. Rockefeller*, 591 F.2d 182, 188 (2d Cir. 1979) (in banking statute, "necessary" did not require investigation to be "absolutely needed" or "inescapable," but need only "arise reasonably and logically out of the main investigation"). The context of "necessary" in the suppression statute fully supports the "useful," "helpful," and "reasonable" constructions because the legislative history references factors that closely parallel the present situation as warranting defense participation. Further, FISA's purpose of balancing civil liberties against national security needs forecloses the complete shutout of defense participation advocated by the government. *See In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (FISA "was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties.").

The legislative history makes clear that adversary proceedings were expected and considered normal where the judicial function expanded beyond the analogy of reviewing a search warrant to determine whether an affidavit established probable cause. Rather than viewing the defense as having no role, Congress sought to establish a "just, effective balance" in determining the "delicate

problems and competing interests" at stake. S. Rep. 604(I), 95th Cong., 1st Sess. 53, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3954; *see* S. Rep. 701, 95th Cong., 1st Sess. 59, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4028. In this context, and citing to pre-FISA case law, the Committee reported that "in some cases" no disclosure would be made, while in "other cases" disclosure would be considered "necessary," because of, "for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order." S. Rep. 604(I), 95th Cong., 1st Sess. 58-59 (footnote omitted); *reprinted in* 1978 U.S.C.C.A.N. 3904, 3959-60; *see* S. Rep. 701, 95th Cong., 1st Sess. 64-65), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4033-44.

In contrast to Congress's expectations, there has never to date been disclosure to the defense in "other cases" under the suppression statute. And, not coincidentally, there has never been a suppression motion granted under § 1806(f). When the government calls upon this Court to follow what it calls "the rule" of nondisclosure (CR 509 at 81-82), what it is really doing is asking the Court to abandon the civil liberties part of the balance by placing the thumb of literal necessity – which arguably never could be met – on the scale to the detriment of the delicate weighing Congress instituted. *See* Jimmy Carter, *Foreign Intelligence Surveillance Act of 1978: Statement on Signing S. 1566 into Law* (Oct. 25, 1978) (FISA sought "the correlation between adequate intelligence to guarantee our Nation's security on the one hand, and the preservation of basic human rights on the other"); *Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence of the United States Senate*, 95th Cong. at 12-13 (1978) (statement of Hon.

Griffin B. Bell) (FISA seeks "a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties").

Especially given the abuses to which Congress was responding in enacting FISA,[18] the context of the statute requires greater flexibility in granting disclosure than the government's "one-in-a-million" standard entails. CR 509 at 81. Indeed, the government's citation to "one-in-a-million" omits that the court referred only to the party's argument, not any holding or dicta of the court itself. *In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 203 (7th Cir. 2003) (noting "the Appellant['s] suggest[ion] at oral argument that this is that one-in-a-million case where disclosure is necessary.") (emphasis added). The government also relies on a treatise that, without supporting citation or analysis, asserts that "necessary" means "required" or "essential." CR 509 at 81-82 (citing 2 David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions*, § 29.3 n.1 (2d ed. 2012)). But even without the foregoing analysis of cases describing "necessary" as flexible and dependent on context, the treatise writers note the restrictive rule of nondisclosure "is, however, somewhat at odds with the explanation of the legislative history." *Id*. at § 31:3 at 263.[19]

Just as the legislative history clearly demonstrates a flexible meaning of "necessary" that anticipates defense involvement under a wide range of circumstances under § 1806(f), companion passages of the legislative history show that Congress intended greater flexibility in its use of

---

[18] William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 Lewis & Clark L. Rev. 1099, 1110 (2007).

[19] The citation provided in the government's brief appears to be in error; the passage cited by the government, as well as the note that such an interpretation is at odds with the legislative history, appears in § 31:3 at the page cited above, not § 29.3.

"necessary" in other parts of the statute. In a discussion of the use in a draft companion statute of "necessary" and "essential" in authorizing surveillance, the Senate Judiciary Committee laid out a range of meaning far less restrictive than the government's purported rule of non-disclosure. S. Rep. 604(I), 95th Cong., 1st Sess. 31, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3933 ("necessary" is more than "useful or convenient," while "essential" is "important and required" but not "of utmost importance or indispensable"). Ultimately, in 50 U.S.C. § 1806(e), the word "necessary" took on the "important and required" meaning – less than the abandoned "essential" – as "intended to mandate a *significant need* be demonstrated by those seeking the surveillance." S. Rep. 701, 95th Cong., 1st Sess. 31, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4000 (emphasis needed). Similarly, "necessary" in 50 U.S.C. § 1801(h)(2) meant that the information "will contribute in a meaningful way to the ability of the recipient of the information to understand the information or assess its importance." H. Conf. Rep. 1720, 95th Cong., 2d Sess. 23 (Oct. 5, 1978).

Under the rule of intra-statutory consistency, the same word or phrase should have the same meaning throughout the statute. *Sullivan v. Stroop*, 496 U.S. 478, 484 (1990). Where "necessary" is being read as to allow governmental surveillance with only a showing of "significant need," and that it will "contribute in a meaningful way," the required balance of civil liberties and national security becomes a sham, implicating due process, in the absence of interpretational reciprocity in favor of the individual citizen in § 1806(f). *See Wardius v. Oregon*, 412 U.S. 470, 477-78 (1973) (statute with express authorization only for government discovery either could be interpreted to provide reciprocal authorization for defense discovery or the discovery provision violated due process). Just as "necessary" means significantly useful or providing a meaningful contribution for

surveillance authorization, the same flexible meaning of "necessary" requires defense participation in adversarial proceedings under the unique facts of this case.

2. The Government's Extensive Submission Of [CLASSIFIED MATERIAL REDACTED] Demonstrates The Unfairness Of Ex Parte Proceedings And The Necessity Of Defense Participation.

Ironically, the government argues that the defense should not be able to mount a facial challenge to the statute, while at the same time refusing to provide the facts on how the statute was applied based on section after section of [CLASSIFIED MATERIAL REDACTED]. Where the relevant materials are sufficiently "complex," disclosure to the defense is necessary to assure reliable adjudication of the motion to suppress. *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982). The present case is unique and complex: the case involves a statute never before adjudicated; the technology involves multiple layers of rapidly evolving and sophisticated electronic devices and practices; and the application involves a cast of government agents and agencies that has failed to provide required disclosures, most notably the pretrial notice of warrantless surveillance.

As the Supreme Court noted in *City of Ontario v. Quon*, the courts should proceed with care when considering the "[r]apid changes in the dynamics" of privacy interests and electronic communication and information transmission technology. 560 U.S. 746, 759 (2010). The government asks the Court to abandon the circumspection Justice Kennedy urged in *Quon*; instead, the government favors decision-making regarding novel electronic surveillance issues based on only one side arguing specific facts and the legal consequences flowing therefrom, where the defense has no opportunity to challenge the government's recitation of events, practices, and policies. The Court should view the extensive redactions in the public pleading as compelling evidence that defense participation is necessary to fair and reliable adjudication of the pending motions.

3. The Government Declaration On National Security Does Not Outweigh The Factors Favoring Adversary Participation As "Necessary" Within The Meaning Of The Statute And As Required By Due Process.

In the discovery briefing, the defense has established strong bases for full adversary proceedings. The government's reliance on the Attorney General's declaration should be tempered by two considerations. First, the government relies on three cases indicating that Article III judges do not have the background or experience to weigh national security issues. CR 509 at 84. Those cases do not adequately consider the generation of litigation in which the federal judiciary has handled thousands on national security cases effectively and safely. *See also Keith*, 407 U.S. at 320 ("We cannot accept the government's argument that internal security matters are too subtle and complex for judicial evaluation.").

Second, the declaration, referencing both "secret" and "top secret" matters, does not address that, in this particular case, the defense team includes lawyers with many years of security clearances and litigation in the area of national security. The certification submitted by the Attorney General regarding national security does not address the core question where the defense does not seek disclosure to anyone other than security-cleared counsel. Such counsel operate under the same statutory obligations of non-disclosure as do executive, judicial, and legislative branch officers and employees with security clearances. We would, moreover, operate under protective orders imposed by the Court. Possession of classified information relevant to national security by attorneys who can only use that information in classified sessions under protective orders cannot pose any more danger to national security than does possession of the same information by an Assistant United States

Attorney.[20] Given the need for advocacy and the availability of counsel with many years of national security clearances, excluding the defense from adversarial proceedings would compromise fairness and the right to due process.

Throughout this reply, the defense points out to the Court the ways in which the government omits critical information from its citation to case authority, selectively quotes from legislative history, and aggressively argues for inroads into traditional Fourth Amendment protections while failing to provide balanced arguments favoring privacy protections. Each one-sided argument illustrates why the programmatic challenge, to comport with the statute and due process, requires full defense participation. "Fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights . . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it." *United States v. James Daniel Good Real Property*, 510 U.S. 42, 55 (1993) (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). The Court should order full discovery to security-cleared counsel to avoid the absurdity of the government's position that only an "as applied" challenge is available, but the government won't tell the defense how the statute was applied.

F. The Defense Has Made A Sufficient Showing For A Hearing Under *Franks v. Delaware*, 438 U.S. 154 (1978).

The government's opposition to a *Franks* hearing does not distinguish the showing already made from the need for adversary access to provide more focused arguments regarding reckless or

[20] The district court grant of defense access in *United States v. Daoud*, CR 490, which included reference to security-cleared defense counsel, has been briefed and is set for oral argument on June 5, 2014. *United States v. Daoud*, No. 14-1284 (7th Cir.).

intentional material omissions or false representations. CR 509 at 87-89. In keeping with that approach, the Court should order a *Franks* hearing based on the evidence already before the Court and grant defense access to material to permit fully informed advocacy. The Supreme Court in *Franks* rejected the government's ultimate position that, because the defense does not know what representations were made, no preliminary showing is possible: "a flat ban on impeachment of veracity could denude the probable-cause requirement of all real meaning." 438 U.S. at 168.

Contrary to the government's claim that the defense should have no role, the *Franks* decision recognized that ex parte proceedings, while necessary at the investigative stage, should give way to adversary proceedings upon an initial post-investigative showing that lawless or reckless conduct needs to be discouraged:

> [T]he hearing before the magistrate not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily ex parte, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an ex parte inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an extended independent examination of the affiant or other witnesses.

Franks, 438 U.S. at 169. In the context of the particular programs involving warrantless surveillance, the defense has made a substantial showing that should trigger both a hearing and defense adversarial participation:

- The Director of National Intelligence, when asked by a congressional committee regarding warrantless surveillance of Americans' electronic communications, including the programs at issue here, unequivocally stated that no such searches wittingly occurred, then, after public disclosures, asserted that he had answered in "the least untruthful manner." Glenn

Kessler, *James Clapper's 'least untruthful' statement to the Senate*, Wash. Post, June 12, 2013.[21]

- The FISC has made repeated findings that the agencies implementing the FAA made misrepresentations to the court and failed to comply with court directives in cases such as *In re Production of Tangible Things from [redacted]*, No. BR 08-13, 2009 WL 9150913, *2 (FISC Mar. 2, 2009) (declassified Sept. 10, 2013), and *[Case Name Redacted]*, No. [docket number redacted], 2011 WL 10945618, *5 (FISC Oct. 3, 2011) (declassified on Aug.21, 2013) (*see generally* CR 489 at 39-41).

- In this case, the government failed to comply with the mandatory pretrial notice to the defense regarding warrantless surveillance under circumstances demonstrating at least reckless disregard for the requirements of § 1806(c).

In the context of defense exclusion from proceedings, which is in stark contrast to the normal defense ability to scour affidavits for material omissions and false statements, the defense has provided compelling reasons to hold a hearing and permit full adversary participation by the defense.

The material omission of the § 1806(c) notice to the Court, as opposed to the defense, is difficult to assess without adversary proceedings. At the outset, the defense indicated lack of knowledge whether the Court received the documents relevant to warrantless surveillance (CR 489 at 1); the government then asserted that the Court did not have the warrantless surveillance documents and should not receive them until the defense filed another suppression motion (CR 493, 497); but now the government claims the Court received the "relevant information" (CR 509 at 6). If the information was the content of the warrantless surveillance but not the fact of the warrantless surveillance, then the Court should consider the failure to give notice to the Court of the warrantless

[21] Available at http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html.

surveillance, in addition to omission of notice to the defense, as a material omission favoring *Franks* adversarial proceedings.

The cases upon which the government relies are easily distinguishable as involving no showing that the government presentation may have been incomplete or overstated and no arguments that defense participation is "necessary" given the contested facts and acknowledged shortcomings in this and other similar national security contexts. To the extent the government is asking the Court to accept a "practical impossibility" standard (*United States v. Kashmiri*, 2010 WL 4705159 (N.D.Ill. 2010)), the Court should emphatically reject such a suggestion as inconsistent with the holding of *Franks*. The Supreme Court's requirement of an initial showing to commence adversarial proceedings necessarily includes consideration of the greater difficulty in presenting a case for review given post-investigation ex parte proceedings, so a less explicit showing triggers the right to *Franks* review. The showing in the present case – especially the material omission of notice to the defense of the warrantless surveillance itself – should easily trigger the adversarial proceedings necessary to assure that the FISA requisites were fairly met by affiants who presented the case for surveillance without material omissions or false representations and without reliance on conclusory statements unsupported by sworn first-hand knowledge of the relevant facts.

G. The Government's Submission Of [CLASSIFIED MATERIAL REDACTED] Regarding The § 215 Telephone Metadata Should Require Both Disclosure And Rulings Regarding Unlawful Electronic Surveillance And Production Of *Brady* Material.

The defense can provide little helpful in reply because virtually the entire government briefing is [CLASSIFIED MATERIAL REDACTED]. CR 509 at 90. Such blanket secrecy militates strongly in favor of permitting security-cleared counsel to participate in adversarial proceedings.

Further, the existence of any telephone metadata, aside from suppression issues, constitutes *Brady* material. CR 489 at 21-23. The defense can also supplement the initial briefing with recent reporting that elaborates on previously undisclosed facts from the FISC regarding challenges to the § 215 program. *See* Charlie Savage, *Phone Company Pushed Back Against N.S.A.'s Data Collection, Court Papers Show*, N.Y. Times, May 15, 2014.

Conclusion

For the foregoing reasons and those stated in the previous briefing, the defense respectfully requests that the Court enter an order granting discovery and full defense participation in the suppression litigation and, with or without such adversary proceedings, granting suppression of the derivative evidence of warrantless surveillance and a new trial.

Dated this 19th day of May, 2014.

/s/ Stephen R. Sady
Stephen R. Sady
Chief Deputy Federal Public Defender

/s/ Steven T. Wax
Steven T. Wax
Federal Public Defender

/s/ Lisa Hay
Lisa Hay
Assistant Federal Public Defender

Mark Ahlemeyer
Research & Writing Attorney