

**No. 14-30217**

---

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

---

**UNITED STATES OF AMERICA,**

**Plaintiff-Appellee,**

**v.**

**MOHAMED OSMAN MOHAMUD,**

**Defendant-Appellant.**

---

**Appeal from the United States District Court  
for the District of Oregon  
Portland Division**

---

**SUPPLEMENTAL BRIEF OF APPELLANT**

---

**Stephen R. Sady  
Chief Deputy Federal Public Defender  
Lisa C. Hay  
Federal Public Defender  
Mark Ahlemeyer  
Assistant Federal Public Defender  
101 SW Main Street, Suite 1700  
Portland, Oregon 97204  
(503) 326-2123**

**Steven Toby Wax  
Attorney at Law  
618 NW Glisan Street, Suite 300  
Portland, Oregon 97208  
(503) 830-7758**

**Attorneys for Defendant-Appellant**

## TABLE OF CONTENTS

	<b>Page</b>
Table of Authorities .....	ii
Introduction .....	1
A. Section 702 Is Facially Unconstitutional Under The Fourth Amendment, The First Amendment, And The Separation Of Powers Doctrine. ....	1
1. Section 702 Violates The Fourth Amendment.....	2
2. Section 702 Violates The First Amendment. ....	9
3. Section 702 Violates The Separation Of Powers Doctrine. ....	11
B. <i>Verdugo-Urquidez</i> Supports Full Application Of The Fourth Amendment To Electronic Surveillance Conducted On American Soil That Intrudes On Americans’ Privacy Rights. ....	14
C. The Fruit Of The Poisonous Tree Doctrine Applies To The Indirect Products Of Electronic Surveillance Including Decisions To Seek A FISA Warrant And To Develop And Implement The Targeted Sting. ....	16
D. The Newly Declassified Information Highlights The Need For This Court To Provide Defense Access To Classified Material As Necessary For Full And Fair Litigation Of This Appeal. ....	18
Conclusion .....	20
Certificate of Compliance .....	21
Certificate of Service .....	22

**TABLE OF AUTHORITIES**

**Page**

**FEDERAL COURT CASES**

*Alderman v. United States*,  
394 U.S. 165 (1969) ..... 18, 18, 20

*Berger v. New York*,  
388 U.S. 41 (1967) ..... 2, 3, 8

*Booker v. United States*,  
525 U.S. 738 (2005) ..... 12

*Boyd v. United States*,  
116 U.S. 616 (1886) ..... 8

*City of Chicago v. Morales*,  
527 U.S. 41 (1999) ..... 10

*City of Los Angeles v. Patel*,  
135 S. Ct. 2443 (2015) ..... 2, 3, 4, 5

*Clapper v. Amnesty Int’l USA*,  
133 S. Ct. 1138 (2013) ..... 8, 11

*Clinton v. City of New York*,  
524 U.S. 417 (1998) ..... 14

*Flast v. Cohen*,  
392 U.S. 83 (1968) ..... 12

*Gibson v. Fla. Legislative Investigation Comm.*,  
372 U.S. 539 (1963) ..... 11

*Grand Jury Subpoena, JK-15-029*,  
828 F.3d 1083 (9th Cir. 2016) ..... 7, 8

*Mistretta v. United States*,  
488 U.S. 361 (1989) ..... 12

*Murray v. United States*,  
487 U.S. 533 (1988) ..... 17

*United States v. Belfield*,  
692 F.2d 141 (D.C. Cir. 1982) ..... 19

*United States v. Mayer*,  
503 F.3d 740 (9th Cir. 2007) ..... 9

*United States v. United States Dist. Ct. for E. Dist. Of Mich.*,  
407 U.S. 297 (1972) ..... 3, 5, 7

*United States v. Verdugo-Urquidez*,  
494 U.S. 259 (1990) ..... 1, 5, 14, 15, 16

*United States v. Williams*,  
553 U.S. 285 (2008) ..... 10

**FEDERAL STATUTORY AUTHORITIES**

50 U.S.C. § 1801(e)(2)(B) (2012) ..... 10

50 U.S.C. § 1806(e) (2012) ..... 9-10

50 U.S.C. § 1806(f) (2012) ..... 18

50 U.S.C. § 1881a(a) (2012) ..... 10

**OTHER**

Richard H. Fallon, Jr., *Fact and Fiction About Facial Challenges*,  
99 Calif. L. Rev. 915 (2011) ..... 3

Walter F. Mondale, Robert A Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*,  
100 Minn. L. Rev. 2251 (2016) ..... 6, 7, 13

## **Introduction**

The Court requested supplemental briefing addressing declassified information provided by the government as it relates to the constitutional challenge to § 702 of the FISA Amendments Act, including: 1) whether the defense is raising a facial challenge to § 702, and if so, under what authority, and 2) the applicability, if any, of *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), including its relevance to the location of the search. The defense contends § 702 is unconstitutional on its face because it independently violates the Fourth Amendment, the First Amendment, and the separation of powers doctrine. The opinion in *Verdugo-Urquidez* supports constitutional privacy protections for private communications of American citizens against seizures and searches conducted within the territory of the United States, as occurred here, because the only Fourth Amendment free zone recognized by the Court in that case required that the search be conducted abroad and that the target not have any “voluntary attachment to the United States.” 494 U.S. at 274-75.

### **A. Section 702 Is Facially Unconstitutional Under The Fourth Amendment, The First Amendment, And The Separation Of Powers Doctrine.**

As elaborated in the opening and reply briefs, the defense asserts that, on its face, § 702 violates three constitutional provisions:

- 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.

Op Br. at 155-62; Reply Br. at 60, 68-91; *see also* Docket No. 98 (referencing the analysis of facial challenges in *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2449-51 (2015)). However, the Court need only reach the facial challenge if the Court has first rejected the narrower arguments that 1) the statute must be construed to incorporate individualized judicial review for United States persons, 2) violation of the statutory notice provision required suppression, and 3) the secondary search of the content of Mr. Mohamud’s electronic communications violated the Fourth Amendment. Op. Br. at 137-55; Reply Br. at 50-68.

*1. Section 702 Violates The Fourth Amendment.*

In denying the motion to suppress evidence derived from warrantless § 702 surveillance, the district court declined to consider a facial challenge under the Fourth Amendment, citing cases suggesting that such challenges were either

disfavored or impermissible in the Fourth Amendment context. ER 193-96. Contrary to the district court's reasoning, the intervening authority of *Patel* makes clear that facial challenges under the Fourth Amendment are not disfavored. 135 S. Ct. at 2449-51. Moreover, the Supreme Court has not hesitated to declare that even complex electronic surveillance statutes facially violate the Fourth Amendment, as in *Berger v. New York*, 388 U.S. 41 (1967), or to review executive assertions of authority to conduct specialized surveillance to protect the national security, as in *United States v. United States Dist. Ct. for E. Dist. Of Mich.*, 407 U.S. 297 (1972) (*Keith*).

As demonstrated in *Patel* and the law review article cited in that opinion, the Supreme Court has allowed facial challenges under an array of constitutional provisions. 135 S. Ct. at 2449; Richard H. Fallon, Jr., *Fact and Fiction About Facial Challenges*, 99 CAL. L. REV. 915 (2011). The *Patel* opinion cited numerous cases in which the Court entertained facial challenges under the Fourth Amendment to statutes authorizing warrantless searches, as well as “numerous occasions” on which the Court declared such statutes facially unconstitutional. 135 S. Ct. at 2450.

The *Patel* opinion also provides guidance regarding the framework for reviewing facial challenges to a provision authorizing warrantless searches and determining whether the statute is unconstitutional “in all applications.” 135 S. Ct.

at 2451. The statute in *Patel* required hotel operators to make certain guest records available to any city police officer on demand. *Id.* at 2447. The dissenting opinion in this Court had concluded that the statute could not be unconstitutional on its face because a police officer’s inspection of hotel records would be constitutional with a warrant or an exception to the warrant requirement. *Id.* at 2449. The Supreme Court rejected this analysis because “its logic would preclude facial relief in every Fourth Amendment challenge to a statute authorizing warrantless searches.” *Id.* at 2451.

Instead, the Court explained that, when assessing whether a statute meets the all-applications standard for a facial challenge, the Court considers “only applications of the statute in which it actually authorizes or prohibits conduct.” *Id.* For statutes authorizing warrantless searches, “the proper focus of the constitutional inquiry is searches that the law actually authorizes, not those for which it is irrelevant.” *Patel*, 135 S. Ct. at 2451. The Court elaborated: “If exigency or a warrant justifies an officer’s search, the subject of the search must permit it to proceed irrespective of whether it is authorized by statute. Statutes authorizing warrantless searches also do not work where the subject of a search has consented.” *Id.* at 2451. Such applications are irrelevant because they “do not involve actual applications of the statute.” *Id.*

In the present case, it is irrelevant to the facial analysis that § 702 would be constitutional as applied to seizures and searches conducted abroad against non-citizens without voluntary connections to the United States because, under *Verdugo-Urquidez*, 494 U.S. at 274, such a search is constitutionally permitted “to proceed irrespective of whether it is authorized by statute.” *Patel*, 135 S. Ct. at 2451. The facial challenge considers only applications of the statute that infringe on constitutionally protected privacy interests. Thus, the question is whether it violates the Fourth Amendment to conduct warrantless surveillance of electronic communications within the United States that extends to the contents of the communications of United States persons.

Analyzed under *Patel*'s framework, § 702, as construed by the government, does not withstand Fourth Amendment scrutiny. The statute authorizes investigators to conduct warrantless searches within the United States of the contents of Americans' electronic communications, with no individualized judicial determination of any level of suspicion. In *Keith*, the Court recognized that electronic surveillance entails “broad and unsuspected governmental incursions into conversational privacy,” necessitating the application of Fourth Amendment safeguards to guard against the risk of executive overreach. 407 U.S. at 313, 317. The lack of any such safeguards in connection with the authority to search

Americans' protected communications renders § 702 unconstitutional in all applications.

Because the newly declassified facts establish that Upstream was not the source of the specific surveillance at issue in this case, the government may argue that the Court need not be concerned with its vast collection, maintenance, and accessing of domestic electronic communications under that program. On the contrary, the fact that § 702 has been interpreted to condone even *broader* applications than occurred here, without traditional Fourth Amendment procedural safeguards, supports the facial overbreadth of the statute in all applications.

Moreover, there is no dispute that § 702 lacks individualized judicial review across all its applications. Former Vice President Walter F. Mondale, who was both a “chairman of the subcommittee that drafted the Church Committee’s final report on domestic intelligence activities” and “instrumental to the passage of the Foreign Intelligence Surveillance Act,” considered § 702’s shift to “bulk adjudication of programmatic surveillance,” and the corresponding lack of individualized judicial review, to be constitutionally “very questionable.” Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2253, 2277-78 (2016). The “most troubling post-9/11 procedural change” was

“the FAA’s (potentially unintentional) amendments to the warrant application procedure,” shifting FISC review from considering pre-search individualized warrant applications to broadly approving targeting and minimization procedures. *Id.* at 2275-76. That shift renders § 702 unconstitutional on its face because it does not retain any provision analogous to traditional judicial review. *See* Reply Br. at 81-82 (chart comparing § 702 with Article III wiretaps and FISA warrants).

In the absence of any prior judicial (or even executive) determination that a foreign power or agent was involved, the holding in *Keith* directly applies. 407 U.S. at 321-22 (“the case only involves the domestic aspects of national security,” with no opinion expressed regarding “the activities of foreign powers or their agents.”). Possession of emails by the government “does not vitiate” the claim of a legitimate expectation of privacy in the content of email and other digital troves. *In re Grand Jury Subpoena, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016). United States citizens “are entitled to the full protection of their privacy” against intrusion by the United States government, even when they communicate with foreigners abroad. *See* Report and Recommendation of the President’s Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, at 148-50 (2013) (Recommendation 12) (Section 702 does not “adequately protect the legitimate privacy interests of United States persons”).

By intruding upon the private writings of countless Americans, with no prior individualized judicial authorization or other protection analogous to the Fourth Amendment, the government's actions essentially constituted the type of general warrant that motivated the Founders to promulgate the Fourth Amendment. *See Boyd v. United States*, 116 U.S. 616, 626-27 (1886) (holding Act of Congress unconstitutional that required production of documents that intruded on “the privacies of life without a warrant”); *Grand Jury Subpoena*, 828 F.3d at 1088 (subpoena calling for all email communications involving seventeen individuals was “analogous . . . to a general warrant, which constitutes an unreasonable search under the Fourth Amendment”). Because § 702 is “too broad in its sweep,” the invasion of constitutionally protected privacy renders the statute unconstitutional. *Berger*, 388 U.S. at 44.<sup>1</sup>

---

<sup>1</sup> The government's prevailing position on standing in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), effectively quashed civil review of § 702's constitutionality, and most § 702 surveillance programs have become known not through government disclosure, but due to the leaks of classified material by Edward Snowden. From 2008 to 2013, the government's narrow and unfounded interpretation of the fruit of the poisonous tree doctrine stymied all review in the criminal suppression context. Thus, a facial challenge to the constitutional validity of § 702 is especially appropriate because the statute would otherwise be effectively insulated from judicial review.

2. *Section 702 Violates The First Amendment.*

Section 702 violates the First Amendment because the breadth and vagueness of its authorization for warrantless surveillance chills Americans' exercise of their First Amendment rights. ER 3128 n.7; ER 3151-53. The district court below did not address the merits of the First Amendment facial challenge. ER 190-92. Instead, relying on *United States v. Mayer*, 503 F.3d 740 (9th Cir. 2007), the court adopted the government's argument that "First Amendment interests in a criminal investigation are protected by the Fourth Amendment, and motions to suppress based on alleged First Amendment violations are analyzed under the Fourth Amendment and the exclusionary rule." ER 191.

The lower court erred by relying on *Mayer* and similar cases because the investigative activities in question in those cases were not conducted under the authority of a particular statute. In *Mayer*, the defendant raised a First Amendment challenge to an officer's actions during an undercover infiltration of a purportedly lawful organization. Because no statute authorized the officer's actions, questions of statutory overbreadth and vagueness were not at issue. Moreover, because FISA specifically provides for suppression of evidence as a remedy in 50 U.S.C. § 1806(e), the First Amendment challenge does not rely on the Fourth Amendment's exclusionary rule.

Section 702 violates the First Amendment because, on its face, it is both overbroad and vague, either of which provides a basis for challenging a statute:

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). 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). Section 702, as construed by the government, permits surveillance of all communications to foreign “persons” for information involving “the conduct of the foreign affairs of the United States.” 50 U.S.C. § 1881a(a) and 1801(e)(2)(B). The communications “to” foreign persons may be communications by Americans from within the United States. Under the government’s interpretation, § 702 permits the government to gather up huge numbers of communications “beyond the statute’s plainly legitimate sweep,” and then review their contents without seeking individualized authorization. Because this large-scale 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. Even without any statutory reference to acquiring, databasing, and then mining the content of Americans' communications, Americans self-censored their electronic communications in response to suspected § 702 surveillance. *See* ER 3152; *Clapper*, 133 S. Ct. at 1164 (Breyer, J., dissenting). Subsequent press reports on leaks and the resulting government admissions about the extent of the programs can only intensify that chilling effect. The subtle stifling effect of surveillance implicates fundamental rights of free speech and free association that “need breathing space to survive.” *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 544 (1963) (citation omitted). In this case, the Court should find § 702 unconstitutional because, through its overbreadth and vagueness, it diminishes protected rights in violation of the First Amendment.

3. *Section 702 Violates The Separation Of Powers Doctrine.*

Section 702 blurs the constitutionally required separation of powers by creating a judicial function that veers too far from the constitutionally mandated role of deciding cases and controversies. By delegating to Article III judges the role of approving surveillance programs in the abstract, rather than adjudicating individual applications under those programs, the § 702 program limits the role of judicial

officers to the non-judicial task of examining proposed executive programs for statutory and constitutional compliance.

The Supreme Court has “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.” *Booker v. United States*, 525 U.S. 738, 755 (2005) (citing *Mistretta v. United States*, 488 U.S. 361, 382 (1989)). 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 the Article III limitation of judicial power to “cases” and “controversies.” “These 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)).

Former Vice President Mondale and his team concluded that § 702 likely “violates Article III of the Constitution” based on two concerns: “FISA Court bulk adjudication of programmatic surveillance arguably constitutes an advisory opinion

in two distinct ways—the court’s decisions are reviewed post-judgment by the executive branch and the issues presented to the court are not yet ripe for review.” 100 MINN. L. REV. at 2298-2301. Approving proposed programs before they are applied or contested is “not a traditional Article III role.” *Id.* at 2299. In addition, FISC decisions approving generic procedures are “one step removed from potential infringements on individual rights” because they leave the government with enough flexibility to apply them “in a variety of ways to specific searches and collected information.” *Id.* Thus, “the court is not deciding an actual controversy[.]” *Id.* As former FISC Judge Robertson told the Privacy And Civil Liberties Oversight Board, authorizing programs under § 702 is better viewed as an administrative function of the Executive Branch that is outside the judicial bailiwick. PCLOB Hearing at 36 (July 9, 2013).

Section 702 also improperly delegates legislative authority to design a program similar to Title III for foreign intelligence surveillance. The legislative branch may not delegate such law-making authority to the executive, especially in the absence of any judicial review of the executive’s application of that program in individual instances. *See 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). This Court should strike down § 702 as exceeding the proper functions of the separate branches of government.

**B. *Verdugo-Urquidez* Supports Full Application Of The Fourth Amendment To Electronic Surveillance Conducted On American Soil That Intrudes On Americans' Privacy Rights.**

The Supreme Court's opinion in *Verdugo-Urquidez* recognized a limited exception to application of the Fourth Amendment to extraterritorial searches involving foreign citizens without voluntary connections to the United States. 494 U.S. at 274. That limited exception derived from the convergence of two lines of reasoning. First, Chief Justice Rehnquist's opinion concluded that "the people" protected under the Fourth Amendment "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." *Id.* at 265. The Court never suggested that foreign citizens located abroad were categorically unprotected. On the contrary, the Court repeatedly formulated the reach of the Fourth Amendment in terms of individuals with sufficient voluntary "connections" to the country. *Id.* at 265, 271, 273.

Second, the Court concluded that the purpose of the Fourth Amendment was to restrict searches and seizures conducted by the United States "in domestic matters." *Id.* at 268. In stating that "domestic matters" excluded "activities of the

United States directed against aliens in foreign territory or international waters,” the Court made clear the essential role of the location of the government’s conduct, explaining that a contrary interpretation would “have significant deleterious consequences for the United States *in conducting activities beyond its boundaries.*” *Id.* at 273 (emphasis added). “Were respondent to prevail, aliens *with no attachment to this country* might well bring actions for damages to remedy claimed violations of the Fourth Amendment *in foreign countries or international waters.*” *Id.* at 274 (emphases added). Further emphasizing the importance of location, the Court pointed out that a warrant “would be a dead letter outside the United States.” *Id.* at 274. For these reasons, the Court announced a limited holding that the Fourth Amendment does not apply when three criteria are met: (1) the search involves “a citizen and resident of” a foreign country, (2) who has “no voluntary attachment to the United States,” and (3) “the place searched [is] located” outside the United States. *Id.* at 274.

Justice Kennedy’s fifth vote and deciding concurrence stated that the key limiting factor was “extraterritorial application of the Constitution” against a non-citizen. *Id.* at 275 (Kennedy, J. concurring). In that context, “adherence to the Fourth Amendment’s warrant requirement [would be] impracticable and anomalous,” whereas Justice Kennedy had “little doubt that full protections of the Fourth

Amendment would apply” if the search had occurred within the United States. *Id.* at 278.

The reasoning of *Verdugo-Urquidez* only supports the conclusion that searches of electronic communications conducted within the territory of the United States implicate full constitutional protections, especially when those searches constitute a suspicionless dragnet that inevitably captures and makes available for government use vast quantities of private communications of American citizens like Mr. Mohamud. The government has conceded (for the first time on appeal) that the location of the present search was within the borders of the United States. Resp. Br. at 109. Moreover, the government has never attempted to make the factual showing that the target of the § 702 surveillance did not have “voluntary connections” to the United States, nor has the defense had the opportunity to controvert any such claims. Any argument that simply targeting any non-citizen abroad exempts even massive privacy intrusions conducted on American soil from constitutional protection misconstrues the reasoning of *Verdugo-Urquidez*.

**C. The Fruit Of The Poisonous Tree Doctrine Applies To The Indirect Products Of Electronic Surveillance Including Decisions To Seek A FISA Warrant And To Develop And Implement The Targeted Sting.**

The declassified information asserts that the government did not introduce email content from warrantless surveillance into evidence at trial. Under the fruit of

the poisonous tree doctrine, that assertion does not end the matter because the relevant inquiry extends to both the direct and indirect products of unlawful searches. *Murray v. United States*, 487 U.S. 533, 542 (1988).

In *Murray*, the police conducted a warrantless inspection of a building that disclosed bales of marijuana. The police later obtained a warrant to search the building, excluding the unlawful observations from its warrant application. The Court held that, to avoid suppression, the decision to seek a warrant must be free from the taint of prior unlawful conduct: “[W]hat counts is whether the actual illegal search had *any effect* in producing the warrant.” *Id.* at 543. n.3 (emphasis added).

The government conceded in its § 702 notice that it used information “derived from” § 702 surveillance in this case. ER 2907-08. The declassified material states that the warrantless surveillance led directly to the government’s decision to seek a FISA warrant. The warrantless surveillance also may have impacted the numerous tactical decisions that culminated in the sting operation against Mr. Mohamud. Any assertion of an independent basis for the decisions leading to and evidence introduced at trial should be subject to an adversarial hearing to resolve the relevant legal and factual questions. *Alderman v. United States*, 394 U.S. 165, 182 (1969).

**D. The Newly Declassified Information Highlights The Need For This Court To Provide Defense Access To Classified Material As Necessary For Full And Fair Litigation Of This Appeal.**

In the motion underlying this appeal, the defense asserted: “[T]his motion seeks suppression of unknown evidence and other uses of information gathered at unknown times by unknown means by unknown persons and agencies operating under unknown protocols.” ER 3116. The information finally declassified by the government pursuant to the Court’s recent order reveals the fact that Upstream was not used in this particular search and that the emails themselves were not introduced at trial. Those scraps do not permit the type of informed advocacy the Supreme Court has recognized as necessary to a fair and reliable adversarial process. *Alderman*, 394 U.S. at 182-84. Indeed, the disclosure highlights the fundamental unfairness of the informational imbalance that has permeated this case.

In the legislative history of FISA, Congress anticipated that the defense would have access to classified material under 50 U.S.C. § 1806(f) in complicated cases where there are “records which include a significant amount of nonforeign intelligence information,” “vague identification of the persons to be surveilled,” and “indications of possible misrepresentation of fact.” *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-70 at 64 (1978)). Each of those factors is present in this case. Section 702 electronic surveillance involves not

just “significant,” but massive amounts of American communications unrelated to foreign intelligence. An undisclosed target is by definition “vague” where the procedures involved no prior individualized review or defense investigation regarding the individual.

And the indications of possible misrepresentations are substantial both in this specific case and more broadly. For example, when Mr. Mohamud challenged the non-FISA seizure and search of his computer hard drive, the litigation generated significant evidence that FBI witnesses’ testimony was incorrect and contradictory. Op. Br. at 132. Further, despite a discovery deadline years before trial, the FBI failed to produce exculpatory emails until the verge of and after commencement of trial. ER 1266-74, 1752-56. Perhaps most tellingly, when the defense requested pretrial disclosure of the existence of precisely the type of warrantless surveillance now under consideration, the government affirmatively and incorrectly represented that it had complied with all discovery obligations. Reply Br. at 52 (citing ER 2965-67). Beyond this specific case, the supervising courts during the relevant epoch noted repeatedly that the entities involved in surveillance provided incorrect information. Op. Br. at 169 (citing ER 443-44, 561, 2955-62).

Given the complex and extensive facts of Mr. Mohamud’s life and his statements—both before and after government operatives contacted him—as well as

the nuanced entrapment defense in this case, the Supreme Court’s admonition in *Alderman* is directly on point: “As the need for adversary inquiry is increased by the complexity of the issues presented for adjudication, and by the consequent inadequacy of ex parte procedures as a means for their accurate resolution, the displacement of well-informed advocacy necessarily becomes less justifiable.” 394 U.S. at 184. Under both the Constitution and the statute, security-cleared counsel should be authorized access to all relevant and helpful classified information to assess “the many and subtle interrelationships which may exist among the facts reflected by these records.” *Id.* at 183-84.

### **Conclusion**

For the foregoing reasons and those stated in previous briefing, the Court should hold that, if the electronic surveillance of Mr. Mohamud complied with the statute, and if the secondary searches do not by themselves provide bases for suppression, the direct and indirect products of the electronic surveillance should be suppressed because the warrantless surveillance of Mr. Mohamud’s communications was unconstitutional.

Respectfully submitted this 3rd day of October, 2016.

/s/ Stephen R. Sady  
Stephen R. Sady  
of Attorneys for Defendant-Appellant

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

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
<b>Plaintiff-Appellee,</b>	)	<b>CA No. 14-30217</b>
	)	
<b>v.</b>	)	
	)	
<b>MOHAMED OSMAN MOHAMUD,</b>	)	
	)	
<b>Defendant-Appellant.</b>	)	

---

**CERTIFICATE OF COMPLIANCE**

---

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the Court’s order dated September 2, 2016, Fed. R. App. P. 32(a)(7)(B), and Fed. R. App. P. 32(a)(5) and (6). The brief has 20 pages, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii), and it has been prepared using Word 2013, 14-point Times New Roman font.

Dated this 3rd day of October, 2016.

*/s/ Stephen R. Sady*  
Stephen R. Sady  
of Attorneys for Defendant-Appellant

**CERTIFICATE OF SERVICE**

I hereby certify that on October 3, 2016, I electronically filed the foregoing Supplemental Brief of Appellant with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

*/s/ Jill C. Dozark*

\_\_\_\_\_  
Jill C. Dozark