Bilal A. Essayli (Sate Bar No. 273441)
D. Andrew Brown (State Bar No. 273430)
ESSAYLI & BROWN LLP
100 Bayview Circle, Suite 100
Newport Beach, California 92660
Telephone: 949.508.2980
Facsimile: 949.508.2981

Attorneys for Abdallah Osseily

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

United States Plaintiff, vs. Abdallah Osseily Defendant.	Case No. 19-CR-00117-JAK **MOTION TO DISCLOSE FISA-RELATED MATERIAL NECESSARY TO LITIGATE MOTIONS FOR DISCOVERY**

The defendant, through his attorneys, respectfully moves this Court for an order compelling disclosure of FISA-related material necessary to litigate motions for discovery and for the suppression of the fruits of FISA activity on the grounds asserted in the accompanying memorandum.

DATED: November 8, 2019

Essayli & Brown LLP

By: /s/ Bilal A. Essayli
Bilal A. Essayli
D. Andrew Brown
Attorneys for Abdallah Osseily

Bilal A. Essayli (Sate Bar No. 273441)
D. Andrew Brown (State Bar No. 273430)
ESSAYLI & BROWN LLP
100 Bayview Circle, Suite 100
Newport Beach, California 92660
Telephone: 949.508.2980
Facsimile: 949.508.2981

Attorneys for Abdallah Osseily

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

United States

Plaintiff,

vs.

Abdallah Osseily

Defendant.

Case No. 19-CR-00117-JAK

MEMORANDUM IN SUPPORT OF MOTION TO DISCLOSE FISA-RELATED MATERIAL NECESSARY TO LITIGATE MOTIONS FOR DISCOVERY

I. INTRODUCTION

Defendant Abdallah Osseily is charged by the National Security Division with two counts of Bank Fraud (18 U.S.C. § 1344) and two derivative counts related to making false statements in his naturalization petition and interview (18 U.S.C. §§ 1425(a) and 1015(a)). Despite being charged by the National Security Division, the government has not alleged or otherwise provided any discovery suggesting that Mr. Osseily has committed any national security related offenses. Rather, the government has charged him with providing an inaccurate tax return in conjunction with two credit applications, in which no financial institutions suffered any losses. During discovery the government produced evidence under a protective order, which strongly suggests that the government was conducting physical and electronic surveillance of Mr. Osseily. The government has not produced any orders or warrants authorizing such electronic surveillance and

the defense reasonably believes that Mr. Osseily was subject to surveillance under the Foreign Intelligence Surveillance Act (FISA).

FISA was enacted in 1978 in an effort to curb abuses regarding surveillance of United States citizens. "The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties." *In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (quoting S. Rep. No. 604, 95th Cong., 2d Sess. 9, reprinted in 1978 U.S.C.C.A.N. 3904, 3910). The defense is seeking the disclosure of FISA orders, applications, minimization procedures, and the fruits of any surveillance so that it can competently litigate pre-trial motions, including the filing of a suppression motion. As explained below, the defense request is based on the Court's authority to order disclosures under FISA, the Fourth and Fifth Amendment, and Federal Rule of Criminal Procedure 16(a)(1).

II. ARGUMENT

A. FISA Authorizes Broad Surveillance And Searches Of United States Citizens But Only If Certain Predicates Are Established

FISA established a unique type of court – one that operates in secret and in which the government is the only entity permitted to appear. FISA authorizes issuance of two types of orders by the Foreign Intelligence Surveillance Court (FISC) – those allowing electronic surveillance and those allowing physical searches. The statutory prerequisites are the same in most respects for both types of intrusions. Any application to the FISC must be made under oath by a federal officer and contain certain information and certifications. 50 U.S.C. §§ 1804 and 1823.[1]

---

[1] In brief, an application for electronic surveillance must: (1) provide the identity of the Federal officer making the application (§ 1804(a)(1)); (2) state the identity or description of the target (§ 804(a)(2)); (3) include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power" (§ 1804(a)(3)(A) and (B)); (4) provide a "statement of proposed minimization procedures" (§ 1804(a)(4)); (5) provide a "description of the nature of the information sought and the type of communications or activities to be subjected to surveillance" (§ 1804(a)(5)); and (6) set forth "certifications" by the Assistant to the President for National Security Affairs, an executive branch (footnote continued)

The statute also requires a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance, including: (1) a statement of facts concerning previous applications that have been made to any judge under this statute and action taken on each previous application; and (2) the specific period of time for which the electronic surveillance is required to be maintained. *Id*. § 1804(a)(7) – (9). The Attorney General must personally review the application and determine that it satisfies the criteria and requirements set forth in the statute. § 1804(d).

Before the FISA court can approve electronic surveillance, it must make findings under § 1805(a): (1) the application was made by a Federal officer and approved by the Attorney General; (2) there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and . . .each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or agent of a foreign power"; (3) the proposed minimization procedure meets the definition of minimization procedures under section 1801(h); and (4) the application contains all statements and certifications required.

In accordance with § 1805(a)(4), if a target is a "United States person," the FISC must find that the "certifications" under § 1804(a)(6)(E) – namely, that the information sought is (i) "the type of foreign intelligence information designated," and (ii) "cannot reasonably be obtained by normal investigative techniques" – are "not clearly erroneous." In contrast to foreigners, United States persons are provided protection for constitutionally protected activity: § 1805(a)(2)(A)

---

official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, stating as follows (§ 1804(a)(6)): (A) the certifying official deems the information sought to be foreign intelligence information; (B) a significant purpose of the surveillance is to obtain foreign intelligence information; (C) such information cannot reasonably be obtained by normal investigative techniques; (D) the type of foreign intelligence information being sought according to the categories describe in section 1801(e) of this title; and (E) the basis for the certification that the information sought is the type of foreign intelligence information designated and such information cannot reasonably be obtained by normal investigative techniques.

provides "[t]hat no United States person may be considered a foreign power solely upon the basis of activities protected by the first amendment."

Critical to operation of FISA and review in this case are the definitions set out in 50 U.S.C. § 1801. "Foreign power" is defined in § 1801(a) to include foreign governments, groups they control, and groups engaged in terrorism. "Agent of a foreign power" is defined by a series of acts that distinguish between "United States person[s]," and "any person other than a United States person." *Compare* 50 U.S.C. § 1801(b)(1) and (2). The types of acts that can support an order for a United States person are far more limited than those that can support an order for other people.

FISA authorizes any "aggrieved person" to move to suppress evidence obtained or derived from electronic surveillance on the grounds that "the information was unlawfully acquired" or "the surveillance was not made in conformity with an order of authorization or approval." § 1806(e)(1) and (2). FISA defines the phrase "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." § 1801(k). The government must provide notice of the fact that surveillance was conducted so that a person may move to suppress the evidence obtained as a result.

B. Disclosure Of The FISA Materials Should Be Made To The Defense Under The FISA Provisions Calling For Disclosure

While some litigation over classified material takes place *ex parte*, Congress, in FISA, recognized the potential necessity for defense access to classified material and participation by an aggrieved party in litigation over the legality of FISA-derived surveillance and searches. Congress and the courts have also recognized that access by the defense to classified material may also be required by the Due Process Clause of the Constitution.

1. Disclosure To The Defense Is Necessary To Make An Accurate Determination Of The Legality Of The Surveillance And Searches.

FISA specifically includes a provision for suppression of unlawfully obtained evidence: When a court determines that electronic surveillance or a physical search "was not lawfully authorized or conducted, it shall . . . suppress the evidence which was unlawfully obtained or derived from the electronic surveillance or physical search of the aggrieved person." 50 U.S.C. §§

1806(g) (electronic surveillance), 1825(h) (physical search). In determining the legality of surveillance, "the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f) (electronic surveillance), § 1825(g) (physical searches). Disclosure is, therefore, warranted when a court needs a defense attorney's input to decide whether the various forms of FISA surveillance used in this case was lawful.

Courts and Congress have identified factors that courts should consider when assessing whether disclosure is "necessary" under § 1806(f): the "complex[ity]" of the legal questions at issue; "indications of possible misrepresentations of fact"; vague identifications; and the volume, scope, complexity of the surveillance materials, or records showing overbroad surveillance.[2] S. Rep. No. 701, 95th Cong., 2d Sess. At 64, reprinted in 1978 U.S.C.C.A.N. 4033; *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987); United States v. Belfield, 692 F.2d 141, 147-48 (D.C. Cir. 1982). Here, defense counsel should be afforded an opportunity to review the application, order, and other related materials to determine if any of the factors described by the Ninth Circuit are implicated. Without defense counsel input, it would be virtually impossible for the Court to determine whether any factual misrepresentations about the defendant were made in the application to FISC. It also appears that the surveillance against Mr. Osseily was long-running and

---

[2] An alarming practice of overbroad surveillance is the government's use of Section 702 of FISA, 50 U.S.C. § 1881a, whereby the government intercepts billions of international communications sent by hundreds of thousands of individuals, including Americans. The government stores these communications in massive databases, retains them for years, and searches them repeatedly for information about Americans—including in domestic criminal investigations. This surveillance takes place inside the United States and with only limited involvement by judges on FISC. All of this surveillance is conducted without a warrant. The FBI's routine queries for Americans' communications are often called "backdoor searches" as they constitute an end around the Fourth Amendment. Media outlets have recently reported on the FBI's abuse of backdoor searches. (*See* Spencer Ackerman, *Secret Court: FBI Warrantless Searches Were Illegal*, The Daily Beast, October 8, 2019, https://www.thedailybeast.com/secret-court-fbi-warrantless-searches-were-illegal). In light of recent documented abuses of this data, it is critical to learn whether any Section 702 information was used to surveil Mr. Osseily, including as a basis for establishing probable cause in any FISA applications in the present case.

may have possibly implicated digital devices, which present novel Forth Amendment questions.

In addition, the government has a history of using warrantless surveillance—including Section 702 surveillance—as the basis for FISA applications. *See James Bamford, THE SHADOW FACTORY*, (Doubleday 2008) at 117 ("By the time the [National Security Agency] operation was up and running in the fall of 2001, between 10 and 20 percent of all the requests coming to the FISA court were tainted by what is known in the legal profession as 'the fruit of the poisonous tree,' that is, the warrantless program."); Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct. 26, 2013 (https://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?module=inline). In order to litigate these complex FISA and non-FISA issues, full disclosure to and involvement by the defense is necessary and appropriate.

2. Defense Input Is Necessary To Address Complex Questions Regarding Statutory Terms And Their Relationship To Criminal Activity.

FISA involves the unique substantive requirement for probable cause of proof that a person is a foreign power or an agent of a foreign power. Instead of directing a judge to find probable cause to believe that the fruits or evidence of a crime may be found, a FISC judge must find that there is probable cause to believe that the target is a foreign power or agent of a foreign power and that the facilities or locations sought to be searched are being used, or are about to be used, by a foreign power or agent of a foreign power. 50 U.S.C. § 1805(a)(2).

The probable cause issues are complex in this case. Under the statutory definitions, no order should have issued under the "foreign power" (50 U.S.C. § 1801(a)) section of the statute because Mr. Osseily does not meet those criteria. Nor, by definition, can he be an agent of a foreign power under § 1801(b)(1) because that section only applies to "any person other than a United States person." 50 U.S.C. § 1801(b)(1) (emphasis added). Thus, any order should have issued under 50 U.S.C. § 1801(b)(2). Precisely what must be found is not, however, clear.

Mr. Osseily is a legal permanent resident who resides in the United States and is, therefore, considered a United States person. The defense has not received any evidence that Mr. Osseily was an agent of a foreign power, let alone that he was involved in any associated criminal activity.

Defense involvement will therefore be necessary to counter assertions made by the government in support of any FISA orders.

3. Defense Involvement Is Necessary To Address Questions Related To The Necessity For Use Of FISA.

In order to limit intrusions under FISA, Congress allowed its use only when the Attorney General certifies "that such information cannot reasonably be obtained by normal investigative procedures." 50 U.S.C. § 1804(a)(6)(C); 1823(a)(6)(C). This provision is similar to that found in 18 U.S.C. § 2518(1)(c) (application must include "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous"). There is scant guidance on the necessity issue under FISA. These questions can be complex, as are the questions of necessity in wiretaps under Title III. *See*, *e.g.*, *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1111-15 (9th Cir. 2005). The defense has received no information from the government to justify the basis for the government's belief that use of FISA was necessary against Mr. Osseily. Disclosure and defense involvement on this important issue is necessary.

4. Defense Involvement Is Necessary To Address Questions Related To Minimization Of The Government's Intrusions.

Under FISA, as under the Title III wiretap statute, the government is required to. demonstrate it has minimized its intrusions.[3] The statute requires three specific types of minimization to protect distinct interests. 50 U.S.C. § 1801. First, by minimizing acquisition, Congress envisioned that surveillance should be discontinued where the target is not a party to the communications. Second, by minimizing retention, Congress intended that information acquired,

---

[3] "[The] minimization procedures are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. If the data is not foreign intelligence information as defined by the statute, the procedures are to ensure that the government does not use the information to identify the target or third party, unless such identification is necessary to properly understand or assess the foreign intelligence information that is collected." *In re Sealed Case*, 310 F.3d at 731 (citing § 1801(h)(2)).

which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible. Third, by minimizing dissemination, Congress intended that even lawfully retained information should only be divulged to those officials with a specific need. *In re Sealed Case*, 310 F.3d at 731. Robust minimization is also constitutionally required. *Berger v. New York*, 388 U.S. 41, 57-58 (1967).

Here, defense counsel input in necessary to determine whether the minimization requirements in place were legally sufficient given the breadth of the surveillance, and whether the procedures were violated. This is especially warranted given the complexity of electronic surveillance techniques used today and recent government violations identified by the FISC. Just last month, the Director of National Intelligence released a redacted FISC opinion finding that the FBI's procedures for accessing Section 702 data violated both the statute and the Fourth Amendment. *See* October 18, 2018 FISC Op.[4] This is not the first transgression identified by the court. In 2017, the FISC identified significant problems with the government's "backdoor searches" of Section 702 data, as well as an array of other violations. *See* April 26, 2017 FISC Op. at 19-23, 68-95. After belatedly disclosing the backdoor-search problem, the NSA struggled for months to "ascertain the scope and causes" of its compliance problems, attributing its failure to "the complexity of the issues involved." *Id*. at 5. This complexity was coupled with, in the FISC's words, "an institutional 'lack of candor' on NSA's part." *Id*. at 19, 67-68 & n.57.[5]

C. Disclosure Is Necessary So That The Defense Can Determine Whether A Basis Exists For A *Franks* Hearing.

The FISA applications may contain intentional or reckless material falsehoods or

---

[4] The declassified FISC opinion can be accessed through the following link: https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf

[5] The government has submitted misleading information to the FISC on a number of other occasions. *See* April 26, 2017 FISC Op. at 30 n.14 (noting other "substantial misrepresentation[s]" regarding "major collection programs"); *In re All Matters Submitted to the FISC*, 218 F. Supp. 2d 611, 620-21 (FISC 2002) (explaining "errors related to misstatements and omissions of material facts" in FISA applications), abrogated on other grounds, In re Sealed Case, 310 F.3d 717.

omissions, and the government's refusal to disclose the applications violates Mr. Osseily's rights under *Franks v. Delaware*, 438 U.S. 154 (1978). In other cases, the government has confessed error relating to "misstatements and omissions of material facts" that it had made in its FISA applications. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISA Ct. 2002), *abrogated on other grounds*, *In re Sealed Case, supra*. Disclosure is therefore necessary so that, based on defense analysis, this Court can conduct a *Franks* hearing at which Mr. Osseily will have the opportunity to inquire into whether the affiants before the FISA court intentionally or recklessly made materially false statements or omitted material information from the FISA applications. In this regard, significant questions are likely to exist regarding the extent to which Mr. Osseily was portrayed as an agent of a foreign power, whether the primary purpose of the electronic surveillance was to obtain evidence of domestic criminal activity or foreign intelligence information, whether the government made the required certifications in the FISA application, and whether it properly obtained extensions of FISA orders.

D. The Fourth And Fifth Amendments Entitle Mr. Osseily To Disclosure Of The Government's Surveillance Techniques.

Disclosure of the surveillance techniques that the government used to carry out its FISA surveillance is essential to Mr. Osseily's due process rights. Due process requires that criminal defendants have a meaningful opportunity to suppress the fruits of illegally acquired evidence. *See Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963); *see also Jencks v. United States*, 353 U.S. 657, 671 (1957) (the government cannot invoke its privileges to "deprive the accused of anything which might be material to his defense"); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 318-24 (1972) (compelling disclosure of surveillance transcripts in a national security case). Because Fifth Amendment due process protections apply in the pre-trial suppression context, circuit courts have held that the government must disclose information to a defendant that could affect the outcome of a suppression hearing. *See United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000).

As the Supreme Court stated in *Alderman*, the defense is in a unique position to evaluate electronic surveillance and assess its relevance to the facts of a case. *Alderman v. United*

States, 394 U.S. 165, 182-84 (1969). As further stated there, "[a]dversary proceedings are a major aspect of our system of justice," and therefore "[a]s 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." *Id*. at 183-84. The Court's ability to represent a defendant is limited by the fact that:

> [a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life.

Alderman, 394 U.S. at 182. The defense perspective is especially critical in cases involving electronic surveillance as "the volume of the material to be examined and the complexity and difficulty of the judgments involved" requires the protections associated with the adversarial process. *Alderman*, 394 U.S. at 182 n.14. Due process requires broad disclosure under FISA.

E. <u>The Federal Rules Of Criminal Procedure Entitle Mr. Osseily To Notice Of The Government's Surveillance Techniques.</u>

The Federal Rules of Criminal Procedure also support Mr. Osseily's request for notice. Under Rule 16(a)(1)(B), Mr. Osseily is expressly entitled to discovery of his relevant recorded statements. Under Rule 16(a)(1)(E), Mr. Osseily is entitled to items "obtained from or belong[ing] to" him, as well as information "material to preparing the defense." *See id*. Because notice of the government's surveillance techniques is essential to Mr. Osseily's ability to seek suppression, this information is plainly "material" under Rule 16(a)(1)(E)(i). *See United States v. Soto-Zuniga*, 837 F.3d 992, 1000-01 (9th Cir. 2016).

III. CONCLUSION

For the forgoing reasons, Mr. Osseily requests the disclosure of FISA materials.