UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	
- v -	:	
	:	**15 Cr. 588 (ER)**
AHMED MOHAMMED EL GAMMAL,	:	
Defendant.	:	

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S PRETRIAL MOTION FOR NOTICE AND DISCOVERY OF SEARCHES, SEIZURES, AND SURVEILLANCE TECHNIQUES, AND THEIR LEGAL BASES

Federal Defenders of New York
Daniel Habib, Esq.
Annalisa Miron, Esq.
Sabrina Shroff, Esq.
Attorneys for Defendant
Ahmed Mohammed El Gammal
52 Duane Street - 10th Floor
New York, NY 10007
Tel.: (212) 417-8769

TO: PREET BHARARA, ESQ.
United States Attorney
Southern District of New York
1 St. Andrew's Plaza
New York, NY 10007
Attn: **Brendan Quigley, Esq. and Negar Tekeei, Esq.**
Assistant United States Attorneys

PRELIMINARY STATEMENT

Ahmed Mohammed El Gammal is charged in a four-count indictment with providing and attempting to provide material support to a foreign terrorist organization, in violation of 18 U.S.C. §§ 2339B and 2 (Count 1); conspiring to do the same, § 2339B (Count 2); aiding and abetting the receipt of military-type training from a foreign terrorist organization, §§ 2339D and 2 (Count 3); and conspiring to receive such training, § 371 (Count 4). Dkt. No. 3 (Indictment). Briefly, the government alleges that El Gammal helped an unindicted co-conspirator, [redacted], travel from the U.S., through Turkey, to Syria, where [redacted] joined the Islamic State in Iraq and the Levant ("ISIL"). Specifically, the government says, El Gammal introduced [redacted] via Facebook to another unindicted co-conspirator, [redacted], who lived in Turkey; and communicated with [redacted] via Facebook while the latter was traveling through Turkey. Dkt. No. 1 (Complaint) ¶¶ 12-16.

El Gammal was arrested and indicted in August 2015. On July 13, 2016 -- almost a year later, and about two months before trial was to begin -- the government provided notice, pursuant to 50 U.S.C. § 1825(d), of its intent to introduce at trial "information obtained and derived from physical searches conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended 50 U.S.C. §§ 1821-29." Dkt. No.

51. [redacted] In a separate motion also filed today, El Gammal asks this Court to suppress the FISA-obtained evidence or, in the alternative, to compel disclosure of the FISA order and associated materials.

The government's acknowledgement that its investigation involved at least one secret search, however, gives rise to the inference that there was more than one. That is true in light of the breadth and progress of the known investigation; the fact that this case involves international communications with both U.S. and non-U.S. citizens abroad; and the multitude of surveillance techniques available to the government in national security investigations. In particular, Rule 16 discovery suggests that the government first learned of El Gammal's involvement in [redacted]'s travel to Syria through means other than an ordinary criminal investigation.

The defense cannot assess the admissibility of evidence whose provenance we do not know. We therefore move to compel notice and discovery of all searches, seizures, and surveillance techniques employed in this case and their legal bases.

BACKGROUND

A. The Government's Investigation Of El Gammal

For more than a year, the government has conducted a searching investigation into El Gammal's personal and professional lives. [redacted] Although the government has identified for many of these searches putative legal bases within the scope of an ordinary criminal investigation, the government has also acknowledged that at least one search [redacted] was conducted pursuant to the extraordinary authority supplied by FISA. Moreover, review of Rule 16 discovery suggests that the government's nonstandard investigation may have swept more broadly. [redacted]

[redacted] is said to have traveled from the U.S. to Turkey, and then to Syria, in January 2015. The government began its investigation of [redacted] in [redacted]. [redacted]

[redacted] Put simply, the government seems to have learned about El Gammal before receiving, in the criminal investigation, the first disclosure that would necessarily have identified him. To be clear, the defense cannot say with certainty that a foreign-intelligence investigation preceded (or supplied information that advanced) the criminal investigation, but the sequence of steps supports that inference.

So does a second fact, [redacted]

[redacted] Thus, the discovery supports the inference that the government had some means of reviewing [redacted] before receiving the Rule 41 warrant return. Again, the defense acknowledges a degree of speculation in its argument, but that is inevitable -- and that is the point of this motion.

B. Search, Seizure, and Surveillance Techniques Generally Available In National-Security Investigations.

The defense's suspicion that the government deployed other extraordinary search techniques finds further support in the availability of myriad tools to collect evidence in national-security investigations, including FISA, the FISA Amendments Act ("FAA"), Executive Order ("EO") 12333, the Warrantless Wiretapping Program/Terrorist Surveillance Program ("TSP"), and National Security Letters ("NSLs").

FISA establishes detailed and complex processes for a variety of information gathering activities. FISA sets forth processes for the collection of electronic information both authorized by the Attorney General without a court order and

with an order issued by the Foreign Intelligence Surveillance Court (FISC) (subchapter I, 50 U.S.C. §§ 1801-1812); for physical searches authorized by the AG without a court order and with a FISC order (subchapter II, 50 U.S.C. §§ 1821-1829); for use of pen registers and trap and trace devices both by the AG without a court order and pursuant to an order issued by the FISC (subchapter III, 50 U.S.C. §§ 1841-1846); and for accessing certain business records with a FISC order (subchapter IV, 50 U.S.C. §§ 1861-1862).

The **FAA** sets forth an extensive and complex statutory scheme detailing the gathering of a wide variety of information concerning certain persons outside the United States. (subchapter VI, 50 U.S.C. §§ 1881, 1881a-1881g). The government uses the FAA to gather telephone and email content disclosed by Internet Service Providers ("PRISM") and for agencies to access directly telephone and internet content ("Upstream Collection").

EO 12333 was originally signed into law by President Reagan in 1981 and "establishes the framework in which our governmental and military agencies are to effectuate the process of gathering foreign intelligence and counterintelligence information, and the manner in which intelligence-gathering functions will be conducted at home and abroad." EO 12333 has been amended many times by other Executive Orders since its original inception. In its briefing to the Supreme Court in Clapper v. Amnesty Int'l

USA, 133 S. Ct. 1138, 1149 (2013), the government alleged "that it can conduct FISA-exempt human and technical surveillance programs that are governed by Executive Order 12333." See Exec. Order No. 12333, §§ 1.4, 2.1–2.5, 3 C.F.R. §§ 202, 210–212 (1981), reprinted as amended, note following 50 U.S.C. § 401, pp. 543, 547–548." In the March 2014 Privacy and Civil Liberties Oversight Board ("PCLOB") hearings on the FAA, Robert Litt, General Counsel, Office of the Director of National Intelligence stated: "Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated. There's a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons." Tr. at 81, PCLOB, Public Hr'g Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (March 19, 2014), available at https://www.pclob.gov/library/20140319-Transcript.pdf. See also Spencer Ackerman, NSA Reformers Dismayed After Privacy Board Vindicates Surveillance Dragnet, The Guardian (July 2, 2014) ("The NSA relies upon [EO 12333] for, among other things, its surreptitious collection of unencrypted information transiting from Google and Yahoo data centers."), available at https://www.theguardian.com/world/2014/jul/02/nsa-surveillance-

government-privacy-board-report. Despite this tool's existence for over thirteen years, no case law exists evaluating its constitutionality.

Shortly after September 11, 2001, President Bush established a **Warrantless Wiretapping Program,** also known as the **Terrorist Surveillance Program** ("TSP") which "authorized the National Security Agency to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States and a participant in the call was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization," Clapper, 133 S. Ct. at 1143-44. The government began obtaining surveillance under TSP in 2001; the program was purportedly discontinued in 2007. The defense is aware of no case evaluating the lawfulness of TSP.

NSLs are another tool used by the government to gather evidence in national security investigations. Five different federal statutory frameworks exist for issuance of National Security Letters. See 18 U.S.C. §§ 2709, 3511; 12 U.S.C. § 3414; 15 U.S.C. §§ 1861u & 1861v; 50 U.S.C. § 436. Section 2709, as amended by the USA PATRIOT Act of 2001, authorizes the FBI to "request the name, address, length of service, and local and long distance toll billing records of a person or entity," if the FBI asserts in writing that the information sought is

"relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b). The provision authorizes the FBI to issue requests to "electronic communication service providers." Id. § 2709(a).

Other possible sources of government surveillance in national security cases documented in the public record include **agency subpoenas**, **mail covers** (39 C.F.R. § 233.3), the **Authorization to Use Military Force (AUMF)**, and other claims of power under the **President's Article II authority as Commander in Chief** (outside of FISA). Given the number of surveillance programs the government concealed for years, the defense motion is not limited to the programs described above or methods publicly acknowledged or disclosed to date. Rather, this Court must ensure that defendants have sufficient notice of any surveillance of their communications or activities so that that they can fairly press their claims before this Court.

C. The Government's Record Of Withholding Notice And Discovery Of Surveillance From Criminal Defendants.

The government has a well-documented history of withholding from criminal defendants notice and discovery concerning novel and legally untested surveillance techniques. For many types of surreptitious surveillance, the government does not believe that it has any obligation to provide notice to defendants at all.

For example, government officials have insisted that "defendants have no right to know" if investigators derived evidence from any of the government's sweeping surveillance activities under Executive Order 12333. See Charlie Savage, Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide, N.Y. Times (Aug. 13, 2014), available at http://nyti.ms/1wPw6l0. In fact, the government appears to maintain a policy against using "incidental 12333 intercepts of Americans as direct evidence in criminal prosecutions against them ... so as not to have to divulge the origins of the evidence in court." Id.

Similarly, the Justice Department for years used so-called "scrubbing" procedures as part of a strategy to ensure that defendants never learned of warrantless wiretapping conducted under the "StellarWind" program and thus had no opportunity to challenge it. See DOJ Office of the Inspector General, A Review of the Department of Justice's Involvement with the President's Surveillance Program (July 2009) ("StellarWind Report"), available at http://nyti.ms/1Yvwvop (pdf pages 415–25, 672–77, 694–96). And the government has recently taken the position that defendants have no right to know when the NSA's bulk call records program contributed to prosecutions -- even though that surveillance program was declared illegal by the Second Circuit after its existence was finally revealed. See Gov't Resp. Br. at 71, United States v. Moalin, No. 13-50572 (9th Cir. Apr. 15,

2016), Dkt. No. 34-1; ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015). In short, the government has repeatedly hidden its most intrusive and controversial surveillance methods from criminal defendants, in order to thwart any adversarial legal challenge.

Even in those instances where notice is expressly required by statute, the government has failed to provide it. The Justice Department failed to provide any defendant with notice of FAA Section 702 surveillance for more than five years, even though Congress made notice of that surveillance compulsory. See 50 U.S.C. §§ 1806(c), 1881e(a). The government apparently did so based on a unilateral and unreviewable determination that its evidence was not "derived from" the surveillance. See Charlie Savage, Door May Open for Challenge to Secret Wiretaps, N.Y. Times (Oct. 16, 2013), available at http://nyti.ms/1r7mbDy (describing how the Justice Department "long used a narrow understanding of what 'derived from' means" to improperly withhold notice from criminal defendants). The government altered course in 2013, but only after public outcry prompted the Solicitor General to conclude that the Justice Department's notice policy "could not be legally justified." Id. Even today, the government refuses to explain how it interprets its duty to give notice of Section 702 surveillance.

Notice and discovery is all the more necessary in light of government efforts to conceal surveillance through the use of

"parallel construction." Parallel construction takes multiple forms, but is broadly designed to make evidence obtained from one source appear as though it was obtained from another. Often, this involves reobtaining the same information using a second, less controversial method, in order to insulate the original method from judicial scrutiny. See John Shiffman & Kristina Cooke, U.S. Directs Agents to Cover Up Program Used to Investigate Americans, Reuters (Aug. 5, 2013), http://reut.rs/1h07Hkl (describing parallel construction as a form of evidence laundering). Thus, emails initially obtained using a controversial foreign intelligence program might be reobtained using an ordinary Rule 41 warrant, leaving both the defendant and the court oblivious as to the original source. Unsurprisingly, parallel construction is routinely accompanied by instructions that agents shall not mention the original surveillance in any court filings, testimony, or legal proceedings. See StellarWind Report at 401 (describing instructions forbidding agents from citing warrantless StellarWind surveillance "in affidavits, court proceedings, subpoenas, or for other legal or judicial purposes"); Jenna McLaughlin, FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers, The Intercept (May 5, 2016), http://bit.ly/24uFSd5 (same for Stingray surveillance). In other instances, agents have even withheld this information from

prosecutors in order to avoid disclosure in court. See Shiffman & Cooke, supra; Brad Heath, FBI Warned Agents Not to Share Tech Secrets with Prosecutors, USA Today (Apr. 20, 2016), http://usat.ly/1W2zIvl.

ARGUMENT

I. The Government Must Provide Notice And Discovery Of The Search, Seizure, And Surveillance Techniques Used In This Case, And Their Legal Bases.

El Gammal's principal argument is straightforward. The Fourth Amendment requires suppression of evidence obtained in, or derived from, an unlawful search. To assert that right, El Gammal must know what searches yielded what evidence.

A. The Fourth And Fifth Amendment Entitle El Gammal To Notice.

The only way to vindicate a criminal defendant's right to suppress illegally acquired evidence is through notice. This suppression right becomes especially important when the government adopts new and intrusive surveillance techniques. By now, it is clear that the government routinely employs legally untested surveillance methods in aid of investigations like this one -- and that it often conceals those methods in order to avoid court review. But the Fourth and Fifth Amendments entitle defendants to challenge the legality of these surveillance techniques and to seek suppression of the derivative evidence. See Wong Sun v. United States, 371 U.S. 471, 486-88 (1963)

(describing "fruit of the poisonous tree" doctrine); Murray v. United States, 487 U.S. 533, 536-37 (1988) (describing right to seek suppression of evidence "derived" from an unlawful search). In addition, El Gammal's right to notice and discovery is also found within the government's obligation under Brady v. Maryland, 373 U.S. 83, 87 (1963), to disclose evidence in its possession that is favorable to the accused, including any information material to a defendant's motion to suppress evidence.

Courts have long found notice a constitutionally required element of surreptitious searches, like wiretaps and sneak-and-peak entries. See, e.g., Berger v. New York, 388 U.S. 41, 60 (1967) (finding wiretapping statute unconstitutional because, among other things, it had "no requirement for notice as do conventional warrants"); United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peak warrant constitutionally defective for its failure to provide explicitly for notice within a reasonable time); United States v. Dalia, 441 U.S. 238, 247-48 (1979) (observing that Title III provided a "constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance"). In response to these rulings, Congress has incorporated express notice provisions into many

surveillance statutes, (see, e.g., 18 U.S.C. § 2518(8)(d) (Title III)), because it recognized that "all authorized interceptions must eventually become known at least to the subject" in order to "insure the community that the techniques are reasonably employed." United States v. Donovan, 429 U.S. 413, 438 (1977) (quoting S. Rep. No. 1097, 90th Cong., 2d Sess., p. 2194 (1968)); see also 50 U.S.C. § 1825(d) (FISA physical search).

But courts can only confront the government's use of new technologies to carry out surreptitious searches in criminal investigations if the government provides notice, as it did in United States v. United States Dist. Ct. (Keith). There, the government responded to the defendant's motion to compel the disclosure of electronic surveillance information in a national-security prosecution by publicly acknowledging that investigators had overheard the defendant's conversations using wiretaps. 407 U.S. 297, 299-300 (1972). Similarly, in Kyllo v. United States, 533 U.S. 27, 29-30 (2001), the defendant received notice that the government's search warrant application relied on evidence gathered using thermal-imaging technology. And in United States v. Jones, 132 S. Ct. 945, 948 (2012), the defendant had notice of the government's use of GPS tracking in order to record his movements. All of these seminal Fourth Amendment decisions would have been impossible if the defendants had not received notice of the government's novel searches.

This is a commonsense point. Due process entitles El Gammal to test, on the facts of this case, whether the government's evidence should be suppressed as fruit of unlawful surveillance. Due process does not leave these questions to the government's sole judgment and discretion. See Alderman v. United States, 394 U.S. 165, 168 (1969) (recounting, in wiretapping challenge, Supreme Court's refusal to "accept the ex parte determination of relevance by the Department of Justice in lieu of adversary proceedings in the District Court"). It would make little sense if the government could predetermine, as part of its notice analysis, difficult or unique legal questions that a defendant would put before the Court -- if only he knew.

Additionally, the government's definition of "derived" evidence is particularly opaque and problematic -- yet notice in many cases turns on that definition. As discussed above, the government has held a "narrow understanding of what 'derived from' means in terms of when it must disclose specifics to defendants" in the context of foreign-intelligence surveillance. See Savage, Door May Open for Challenge to Secret Wiretaps, supra. If the government is defining "derived" evidence more narrowly than the Constitution permits, and withholding notice on that basis, then it is concealing the underlying sources of its evidence and insulating them from judicial review. As explained above, the government similarly distorts the meaning

of "derived" evidence when it engages in "parallel construction" in order to conceal the course of its underlying investigation. Evidence laundering strategies designed to obscure the government's use of novel or controversial forms of surveillance do not comport with the Fourth Amendment or due process.

Indeed, the Supreme Court has repeatedly made clear that when the government chooses to criminally prosecute someone, it may not keep the sources of its evidence secret: "[T]he Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense." Jencks v. United States, 353 U.S. 657, 670–71 (1957). Simply put, the government may not have it both ways -- its secrecy and its prosecution -- when an individual's liberty is at stake. Due process requires not only notice to a defendant, but may also call for disclosure of underlying surveillance applications or intercepts. This is why the Supreme Court has previously compelled the government to turn over records of wiretapped conversations in a national security case, even as the government threatened to abandon the prosecution if required to

disclose them. See Keith, 407 U.S. at 318-24. The government is bound by that same choice here, wherever it has relied in whole or in part on undisclosed surveillance programs in the course of its investigation.

B. 18 U.S.C. § 3504 Entitles El Gammal To Notice.

Congress has also provided a right to notice of electronic surveillance by statute. Under 18 U.S.C. § 3504, if a party in a proceeding before any court claims that "evidence is inadmissible" because "it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act" then the government must "affirm or deny the occurrence of the alleged unlawful act." An "unlawful act" is "the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto." Id. § 3504(b).

The government has recognized that 18 U.S.C. § 3504 requires the "affirmance or denial of the fact of electronic surveillance, even if the government believes it was lawful." 2 David J. Kris & Douglas Wilson, National Security Investigations and Prosecutions 237 n.2 (2012). Because a defendant will have only limited information about the government's undisclosed surveillance, "the allegations of unlawful wiretapping required to trigger the government's

obligation to respond by affidavit or sworn testimony need only set forth a colorable claim." In re Millow, 529 F.2d 770, 774 (2d Cir. 1976). "Although the claim need not be particularized, it may not be based upon mere suspicion but must at least appear to have a 'colorable' basis before it may function to trigger the government's obligation to respond under § 3504." United States v. Pacella, 622 F.2d 640, 643 (2d Cir. 1980) (quoting United States v. Yanagita, 552 F.2d 940, 943 (2d Cir. 1977)). Here, the government has acknowledged executing one extraordinary search against El Gammal. As explained above, several additional factors -- including the breadth of the investigation and the inference that other nonstandard searches may have occurred, the presence of international communications involving foreign citizens, and the many tools available to the government in national-security cases -- combine to establish a colorable claim.

C. Rules 12 And 16 Entitle El Gammal To Notice.

Fed. R. Crim. P. 12(b)(3)(C) and 16(a)(1)(E)(i) also support El Gammal's request for notice and discovery of the government's surveillance techniques because such information is necessary to prepare a motion to suppress. Indeed, the defense's request falls squarely within Rule 16(a)(1)(E)(i)'s materiality requirement because a suppression motion directly implicates the government's ability to prove that he committed

the crimes charged. See United States v. Armstrong, 517 U.S. 456, 462 (1996) (holding that Rule 16(a)(1)(c), the predecessor to Rule 16(a)(1)(E)(i), applies to "shield" claims that "refute the Government's arguments that the defendant committed the crime charged"). Because El Gammal cannot meaningfully respond to the evidence comprising the government's case in chief without knowing the extent of its surreptitious searches and seizures, he is entitled to notice and discovery. Id. at 462 (defining the term "defense" in Rule 16 as the "defendant's response to the Government's case in chief").

D. The Government Must Disclose Any Searches, Seizures, Or Surveillance That Resulted In Evidence Relied Upon in Search Warrant Affidavits.

Alternatively, the government has an obligation to disclose information that it expressly relied upon in seeking its Rule 41 search warrants. Once the government decides it will introduce the fruits of a search warrant at trial, [redacted] a defendant has a right to receive information material to examining the legality of the search. Such a right necessarily includes the ability to challenge the information upon which the government relied in the search warrant affidavit. See Franks v. Delaware, 438 U.S. 154, 155–56 (1978) (recognizing a defendant's Fourth Amendment right to challenge affiant's statements upon a preliminary showing). To imbue that right

with meaning, a defendant also has a right to information about the sources of the information relied on by the government in the search warrant affidavit. See Roviaro v. United States, 353 U.S. 53, 59 (1957) (setting forth test for a defendant to obtaining disclosure relating to a confidential informant). The government must comply with the Fourth Amendment and the Due Process Clause by disclosing to a defendant the sources of the information relied upon in each search warrant affidavit. Franks and Roviaro instruct that the government may not shield from a defendant information material to evaluating the validity of a search warrant while at the same time relying on that information to obtain a warrant. The government can omit information from a search warrant application if it desires to keep the information secret. But once the government includes such information in a Rule 41 warrant affidavit, information about how the government obtained evidence in the affidavit is thus material the admissibility of evidence. The government must provide that information to a criminal defendant. See Fed. R. Crim. P. 16(a)(1)(E)(i).

CONCLUSION

For the reasons stated, this Court should order the government to disclose all searches, seizures, and surveillance techniques employed in this case, as well as their legal bases.

Dated: New York, New York
August 12, 2016

Respectfully submitted,
Federal Defenders of New York

/s/ Daniel Habib, Esq.
Daniel Habib, Esq.
Annalisa Miron, Esq.
Sabrina Shroff, Esq.
Attorneys for Defendant
Ahmed Mohammed El Gammal
52 Duane Street - 10th Floor
New York, NY 10007
Tel.: (212) 417-8769