IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,

Plaintiff

v.

Mohammed Zaki Amawi, et al.,

Defendant

Case No. 3:06CR719

ORDER

This is a criminal case in which former codefendants, Zubair and Kahleel Ahmed, filed a motion seeking disclosure and suppression of evidence obtained from surveillance conducted pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq. [FISA] [Doc. 324]. The defendant Marwan El-Hindi filed a similar motion. [Doc. 380], which incorporates the Ahmed motion.

Defendants based their motions on the fact that, during a detention hearing following the post-indictment arrest of the Ahmeds, the government disclosed that it had FISA-derived evidence pertinent to those proceedings.[1]

In an earlier ruling, I held that it was not necessary to decide the issues raised in these motions because the government, which has not acknowledged that it has FISA-derived evidence, has stated that it will not offer any such evidence in its case in chief. The pending motions were, accordingly, in my view, moot. [Doc. 557]. The government, during a proceeding relating to other

[1] The government has not acknowledged that either of the Ahmeds or any of the defendants in this case were the targets of such surveillance or were intercepted during the course of any such surveillance directed against third parties.

matters, suggested that that ruling was not entirely correct, in that the motions seek not just suppression, but disclosure as well. That contention being well-taken, this opinion will adjudicate the defendant El-Hindi's demand, in which codefendants Amawi and Mazloum have joined, for production of any FISA-derived evidence.

The government's opposition argues that disclosure of FISA-derived evidence (and the applications and orders pursuant to which any FISA surveillance may have been conducted) is neither permitted nor justified. It asserts that review of the FISA materials sought by defendants can, and typically does, occur *ex parte* and *in camera*.

In support of its opposition to the pending motions, the government submitted a sealed exhibit containing classified and other documents for *in camera, ex parte* review.[2] The government also publicly filed a redacted version of its opposition, in which classified material had been deleted.

For the reasons that follow, the request to disclose shall be denied.[3]

Background

1. FISA Applications, Orders and Procedures

FISA authorizes the Foreign Intelligence Surveillance Court [FISC] to issue orders allowing officers of the Executive Branch to use electronic surveillance and physical searches, *inter alia*,

---

[2] The classified documents include a memorandum of law, certified copies of the relevant FISA materials; and a classified Declaration by an FBI Supervisory Special Agent as to the manner in which the FISA collection was conducted. The submission also included an unclassified Declaration and Claim of Privilege by the Acting Attorney General and a classified Declaration by an Assistant Director of the Federal Bureau of Investigation in support of that Declaration and Claim of Privilege. The government has also filed an unclassified version of its classified memorandum of law.

[3] My ruling does not, of course, preclude the Ahmeds, who have been separately indicted, from renewing their motion when opportune to do so.

against agents of an organization engaged in international terrorism. Where such surveillance is directed at "United States Persons," which, under § 1801(i) "means a citizen of the United States, an alien lawfully admitted for permanent residence," the surveillance, as a general rule, can only occur pursuant to an order from the FISC.[4]

Before the Executive Branch submits an application to the FISC for consideration, it must obtain certifications from the Attorney General [or certain other designated high-ranking officials], 50 U.S.C. §§ 1804(a), 1823(a), and, as well, a high-ranking official with either national security or defense responsibilities. 50 U.S.C. §§ 1804(a)(7), 1823(a)(7). The FISC cannot consider an application for FISA surveillance, or issue an order authorizing FISA surveillance, unless these officers have confirmed that they have conducted the requisite reviews.

The purpose of the FISA order and surveillance is to obtain "foreign intelligence information," which includes, *inter alia*, information that "relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . actual or potential attack or other grave hostile acts of . . . an agent of a foreign power [and/or] . . . international terrorism by a . . . an agent of a foreign power." 50 U.S.C. § 1801(e).

A FISA application for electronic surveillance must contain, *inter alia*:

- "the identity, if known, or a description of the specific target of the electronic surveillance;"
- a statement of the facts and circumstances supporting the belief that the target "is a foreign power or an agent of a foreign power" and that each facility or place "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;"
- a statement of the proposed minimization procedures to be followed; and

---

[4] There is no dispute that the defendants are "United States Persons" as defined in § 1801)(i).

- a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

- the manner or means by which the electronic surveillance or physical search will be effected and a statement whether physical entry is required to effect the electronic surveillance;

- the facts concerning and the action taken on all previous FISA applications involving the target, facilities, places, premises or property specified in the application; and

- the duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(11).[5]

After the Attorney General certifies the application, the Department of Justice submits it to the FISC for review. That court can issue an order authorizing a FISA surveillance or search on finding, *inter alia*:

- the application has been made by a "Federal officer" and has been "approved" by the Attorney General;

- 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 that 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, or that the premises or property to be searched is owned, used, possessed by or in transit to or from an agent of a foreign power or a foreign power;

- proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) or 50 U.S.C. § 1821(4) (physical search); and

---

[5] Applications for physical searches under FISA must contain substantially similar information. 50 U.S.C. § 1823(a)(1)-(9). Such applications must, though, show probable cause that "the premises or property to be searched contains foreign intelligence information," 50 U.S.C. § 1823(a)(4)(B), and state "what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information." *See* 50 U.S.C. § 1823(a)(8).

- the application contains all of the statements and certifications required by section 1804 or section 1823 and, if the target is a United States person, the certifications are not clearly erroneous on the basis of the statement made under § 1804(a)(7)(E) or § 1823(a)(7)(E), and any other information furnished under § 1804(d) or § 1823(c).

See 50 U.S.C. §§ 1805(a)(1)-(5), 1824(a)(1)-(5) (emphasis supplied).

The definitions of "foreign power" include "a group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. §§ 1801(a)(4). With regard to "United States persons," the statute states that "agent of a foreign power" means "any person who knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." 50 U.S.C. § 1801(b)(2)(C).

FISA defines "international terrorism" as activities that:

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
>
> (2) appear to be intended —
>
> > (A) to intimidate or coerce a civilian population;
> >
> > (B) to influence the policy of a government by intimidation or coercion; or
> >
> > (C) to affect the conduct of a government by assassination or kidnaping; and
>
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

50 U.S.C. § 1801(c) (electronic surveillance).

The FISC issues its orders *ex parte*. 50 U.S.C. §§ 1805(a), 1824(a)(1). FISA orders must

specify:

- the identity of the target of electronic surveillance or physical search; the nature and location of the facilities or places at which the electronic surveillance will be directed, or of each of the premises or property to be searched;

- the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance, or the type of information, material or property to be seized, altered or reproduced;

- the means by which electronic surveillance will be effectuated and whether physical entry will be necessary to effectuate the surveillance, or a statement of the manner in which the physical search will be conducted;

- the authorized scope of the coverage of the physical search, or the period of time during which the electronic surveillance is approved; and

- the applicable minimization procedures.

50 U.S.C. §§ 1805(b)(1)(A)-(F), 1824(c)(1)(A)-(E).

FISA surveillance of United States persons can last for ninety days, 50 U.S.C. §§ 1805(e)(1), 1824(d)(1), and be extended on filing and approval of another application and issuance of another order complying with the requirements of FISA. 50 U.S.C. §§ 1805(e)(2), 1824(d)(2).

The statute requires the Attorney General to adopt minimization procedures for acquiring, retaining, and disseminating FISA-obtained information. These procedures must be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4).

The minimization procedures can include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be

committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

Before the government can use such information, the Attorney General must have provided advance authorization. *See* 50 U.S.C. §§ 1806(b), 1825(c). An "aggrieved person"[6] can move to suppress FISA-derived evidence which the government seeks to use in a criminal case. The basis for a suppression motion can be that the government acquired the information unlawfully; or it failed to conduct the FISA surveillance or search in conformity with the FISA order. 50 U.S.C. §§ 1806(e), 1825(f).

2. Limitation on Disclosure of FISA Materials

FISA provides that if "the Attorney General files an affidavit under oath that disclosure or an adversary [suppression] hearing would harm the national security of the United States," a district court shall conduct an *in camera* and *ex parte* review, "notwithstanding any other law," of "the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1825(g).

Where the Attorney General has filed such affidavit, as the Acting Attorney General has in this case, FISA precludes the district court from disclosing the FISA application, order, or other materials relating to the surveillance [or physical search] unless such disclosure "is necessary to

---

[6] An "aggrieved person" is a "person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), or a "person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2).

make an accurate determination of the legality of the surveillance [or physical search]." 50 U.S.C. §§ 1806(f), 1825(g). Where, on the basis of what it receives from the government *in camera* and under seal, a district court concludes that it can determine whether a FISA surveillance and search was lawful, it may not order disclosure of any of the FISA materials. *See U.S. v. Damrah*, 412 F.3d 618, 624-25 (6th Cir. 2005) (upholding constitutionality of these procedures and affirming district court's denial of motion to compel production of FISA materials and to suppress FISA evidence).

Once the court determines on the basis of its *in camera* review that the FISA surveillance was lawful, it must deny defendants' motions for suppression and disclosure of the FISA material and the fruits of the FISA collection, "except to the extent that due process requires discovery or disclosure." 50 U.S.C. §§1806(g), §1825(h). Discovery of FISA-derived evidence is limited to that required under the doctrine of *Brady v. Maryland*, 373 U.S. 83 (1963). *See, e.g., U.S. v. Thomson*, 752 F.Supp. 75, 82-83 (W.D.N.Y. 1990).

A. Attorney General's Affidavit

As noted, the materials submitted by the government in support of its opposition to the defendants' motion include a declaration by the Acting Attorney General, in which he states that disclosure or an adversary hearing would harm national security. Under FISA, I cannot second-guess that representation. *See, e.g., In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 205 (7th Cir. 2003) (Congress intended that reviewing court "have no greater authority to second-guess the executive branch's certifications than has the FISA judge") (citing *U.S. v. Duggan*, 743 F.2d 59, 77 (2d Cir.1984)). Accordingly, I conduct my review of the lawfulness of the FISA surveillance, including the adequacy of the Attorney General's affidavit regarding the basis for nondisclosure of FISA material, *in camera*, without the prior disclosure of the FISA material to,

or participation of, defendants' counsel.[7]

Determination of the issue of disclosure of FISA materials and derived evidence typically occurs in the context of a motion to suppress, such as that filed by the defendants, but which I have, as noted, overruled, without prejudice, as moot.

The defendants made their instant request for disclosure in conjunction with their demand for suppression. That request, if read narrowly and literally, is likewise moot, as there is not now and may never be a review of the lawfulness of any FISA-derived evidence.[8] Nonetheless, viewing their demand as one for discovery on whatever basis might be available to them, I have reviewed the Acting Attorney General's affidavit with an eye to any other possible basis for disclosure, including the *Brady* doctrine. *Brady v. Maryland*, 373 U.S. 83 (1963).[9]

On review of the classified materials submitted under seal for *in camera* review, I have no doubt that the Attorney General's declaration is well-taken. The FISA-related materials contain considerable operational and technical information [much of it required by the statute] about how FISA orders are implemented. Were that information to become known, the ability to use those operational methods and technical means could be impaired, with potential adverse consequences

---

[7] Having accepted the statements in the Attorney General's declaration as a basis for declining the defendants' request for disclosure of FISA materials, I need not consider the alternate basis – national security privilege – that he asserts.

[8] Such review will be necessary only if the government states an intention to use any such evidence in rebuttal. *See* Doc. 557.

[9] I have conducted my review notwithstanding my conviction that it is inappropriate to order pretrial disclosure of *Brady* material. Ordering the government to do that which the Constitution already commands would hardly serve a useful purpose if the government were of a mind to ignore its constitutionally mandated duties. *See U.S. v. Skeddle*, 176 F.R.D. 258, 260 n.1 (N.D.Ohio 1997).

on the government's ability to obtain useful foreign intelligence information, and, in turn, on national security.[10] In addition, I see nothing in those materials that comes within the government's *Brady* obligations, or otherwise could properly provide a basis for granting the defendants' motion for disclosure.

Conclusion

For the foregoing reasons, it is hereby

ORDERED THAT defendants' motion for disclosure of FISA materials and FISA-derived evidence, if any, be, and the same hereby is denied.

---

[10] This is in no way whatsoever to say that I perceive any direct risk whatsoever of these consequences from disclosure to defendants' counsel, in whose integrity and fidelity to their obligations I have complete confidence. There is, however, always an indirect risk, however slight, of inadvertent disclosure, no matter how strenuous the efforts to contain the scope of disclosure. "Need to know," *see* Executive Order 13292, § 6.1(z) (requiring that a "need to know" determination be made prior to the disclosure of classified information to anyone, including those who possess a security clearance), is a practical, effective, and universally accepted, understood, and applied standard. Indeed, it is a standard that operates, according to my experience as a member of the FISC, informally among the Judges of the that court. That we don't talk with each other about things we know about unless we need to do so evidences, obviously, no concern about the integrity and discretion of our colleagues. The same is true here: by noting that the risk of exposure increases in tandem with and proportionately to the extent of disclosure, I harbor no concern that counsel would fail to abide by any and all restrictions that would accompany disclosure of classified material, were I to be granting their request for such disclosure to them.

I make the observations to which I append this footnote simply to confirm, as the Acting Attorney General has declared, that, were some of the classified information in the FISA applications to become known to those who should not know it, it is indisputable that national security would be placed at undesirable and unacceptable risk. And, to the extent that I might question whether disclosure of other, apparently less sensitive but still classified information would create any real risk to national security, I should be very cautious about substituting my judgment for that of those who know more than I, and whose job it is to know better than I, just what those risks might be. *See United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods.").

So ordered.

s/James G. Carr
James G. Carr
Chief Judge