

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

Filed with the Classified
Information Security Officer
CISO M. White
Date 5/9/2017

UNITED STATES,)

v.)

1:16-cr-265 (LMB)

NICHOLAS YOUNG,)

Defendant.)

MEMORANDUM OPINION

Defendant Nicholas Young is awaiting trial for one count of attempting to provide material support to a designated foreign terrorist organization (“FTO”), namely the Islamic State of Iraq and the Levant (“ISIL”), in violation of 18 U.S.C. § 2339B, and three counts of obstruction of justice, in violation of 18 U.S.C. § 1512. [Dkt. No. 38]. Specifically, Count One alleges that between December 3, 2015 and August 2, 2016, Young “attempted to provide misleading information to the FBI in order to protect [an associate’s] ability to avoid capture and continue to serve ISIL” and “provided gift cards (and gift codes), which he understood were used by ISIL to facilitate recruitment, “to [his associate] understanding that the funds held in those cards would be provided to ISIL and used by ISIL to facilitate recruitment of others to join ISIL.” *Id.* at 1. The details of the alleged activity are set forth in a previous Memorandum Opinion regarding defendant’s motion to suppress evidence obtained from Rule 41 search warrants [Dkt. No. 91], which was denied [Dkt. No. 78].

On January 17, 2017, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the government provided notice to Young and the Court that it “intends to offer into evidence, or otherwise use or disclose in any proceedings in [this case], information obtained or derived from electronic surveillance and physical searches conducted pursuant to the Foreign Intelligence Surveillance

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

Act of 1978 ('FISA'), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829." [Dkt. No. 60]. The underlying FISA application(s) and order(s) are classified. On January 31, 2017, without seeing the relevant FISA application(s), defendant filed a Motion for Disclosure of FISA-Related Material and/or to Suppress the Fruits or Derivatives of Electronic Surveillance and Physical Search Pursuant to FISA ("FISA Motion"). [Dkt. No. 65]. Defendant argues that the underlying FISA application(s) and other materials should be disclosed to defense counsel so that counsel can provide effective assistance, emphasizing that the relevant statutory provisions permit such disclosure under certain circumstances and claiming that ex parte proceedings are "anathema" to adversarial proceedings. Def. Mem., [Dkt. No. 62-1] at 8-15. In addition, defendant claims that the government's FISA evidence should be suppressed because the defendant was neither the "agent of a foreign power" nor engaged in "international terrorism," and because the FISA applications were "likely improperly predicated on protected First Amendment activities," normal investigative techniques could have been employed, and the required minimization procedures "may not have been followed." Def. Mem. at 15-22.

The government has filed a classified opposition brief and the relevant FISA materials have been submitted in camera, ex parte, and under seal. [Dkt. No. 83]. An unclassified and redacted version of its opposition brief has also been filed. [Dkt. No. 82-1]. The government concurrently filed an affidavit signed by the Attorney General claiming that disclosure or an adversary hearing would harm the national security of the United States, [Dkt. No. 82], and argues that pursuant to 50 U.S.C. §§ 1806(f) and 1825(g) the Court "must conduct an in camera, ex parte review of the documents relevant to the defendant's motion." Gov. Opp. at 2. Substantively, the government argues that "the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted in compliance with

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

FISA” and disclosure to the defendant is not authorized “because the Court can make an accurate determination regarding legality without disclosing the FISA materials or portions thereof.” *Gov. Opp.* at 2.

Defendant submitted a reply brief entitled “Classified Reply in Support of Motion for Disclosure of FISA-Related Material and/or to Suppress the Fruits or Derivatives of Electronic Surveillance and Physical Search Pursuant to FISA; and Motion for Reconsideration of March 10, 2017 Order.” [Dkt. No. 84]. The motion to reconsider pertains to a non-FISA issue and has been dealt with in a separate opinion. [Dkt. No. 91]. For the reasons that follow, defendant’s FISA Motion will be denied.

I. OVERVIEW OF FISA

FISA was enacted in 1978 to establish a framework under which the executive branch “could conduct electronic surveillance for foreign intelligence purposes without violating the rights of citizens.” *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (en banc), vacated on other grounds, 543 U.S. 1097 (2005).¹ Under FISA, the Chief Justice of the United States designates eleven United States District Judges to sit as members of the Foreign Intelligence Surveillance Court (“FISC”). *See* 50 U.S.C. § 1803(a)(1). Subject to certain exceptions,² the executive branch must receive advance approval from a FISC judge for all electronic surveillance of a foreign power or its agents. *Hammoud*, 381 F.3d at 332. To secure such approval, the government must file an *ex parte*, under seal application with the FISC. 50

¹ Although FISA initially only pertained to electronic surveillance, *see* 50 U.S.C. §§ 1801-1812, it has since been expanded to include physical searches, *see* 50 U.S.C. §§ 1821-1829.

² The Attorney General may issue an emergency order authorizing FISA surveillance under certain circumstances, *see* 50 U.S.C. §§ 1805(e)(1); however, the government must submit an application to a FISC judge “as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance,” *id.* *See also* 50 U.S.C. § 1824(e)(1).

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

U.S.C. § 1804. For electronic surveillance,³ this application must be approved by the Attorney General and include, among other things, the identity or a description of the target of the electronic surveillance and a statement of the facts and circumstances supporting probable cause to believe that “(A) the target of the electronic surveillance is a foreign power⁴ or an agent of a foreign power;⁵ and (B) 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,” as well as a detailed description of the information sought and the types of communication or activities subject to surveillance. See 50 U.S.C. § 1804(a)(2), (3), (5). In addition, the application must contain a certification from high-ranking executive branch official stating that “the certifying official deems the information sought to be foreign intelligence information,” “that a significant purpose of the surveillance is to obtain foreign intelligence information,” and “that

³ The requirements for physical surveillance are similar but include additional requirements that the application detail the facts and circumstances that justify an applicant’s belief that “the premises or property to be searched contains foreign intelligence information” and that each “premise or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from” the target. 50 U.S.C. § 1823(a)(1)–(8), (a)(3)(B), (C).

⁴ A “foreign power” is defined as a “foreign government or component,” entity controlled by a foreign government, “group engaged in international terrorism or activities in preparation therefor,” “foreign-based political organization,” or entity that is “engaged in the international proliferation of weapons of mass destruction.” 50 U.S.C. §§ 1801(a)(1)–(7), 1821(1).

⁵ A non-U.S. person is an “agent of a foreign power” if he/she “acts in the United States as an officer or employee of a foreign power,” “acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States,” or “engages in international terrorism” or “international proliferation of weapons of mass destruction” or activities in preparation therefor. 50 U.S.C. § 1801(b)(1). The definition of “agent of a foreign power” is similar for a U.S. person but the relevant behavior must be done “knowingly.” See 50 U.S.C. § 1801(b)(2).

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

such information cannot reasonably be obtained by normal investigative techniques.” *Id.* at §§ 1804(a)(6), 1823(a)(6).⁶

A FISC judge may issue an order authorizing FISA surveillance only upon concluding “that there is probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power, that proposed minimization procedures are sufficient under the terms of the statute, that the certifications required by § 1804 have been made, and that the certifications are not clearly erroneous.” United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000). The order authorizing FISA surveillance “must describe the target, the information sought, and the means of acquiring such information” and also “set forth the period of time during which the electronic surveillance or physical searches are approved, which is generally ninety days or until the objective of the electronic surveillance or physical search has been achieved.” United States v. Rosen, 447 F. Supp. 2d 538, 544 (E.D. Va. 2006).

“[O]nce the electronic surveillance or the physical search has been approved, the government must apply the specific minimization procedures contained in the application to the FISC.” *Id.* at 550. Although the specific minimization procedures contained in each application are classified, the statute requires that such minimization procedures 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,

⁶ As defined by the statute “foreign intelligence information” is that which “relates to . . . the ability of the United States to protect against . . . attack or other grave hostile acts of a foreign power [or agent thereof]; sabotage, international terrorism, or . . . clandestine intelligence activities by . . . a foreign power [or agent thereof].” 50 U.S.C. §§ 1801(e)(1), 1821(1). It also includes “information with respect to a foreign power or territory that relates to . . . the national defense[,] security . . . [, or] foreign affairs of the United States.” *Id.* at § 1801(e)(2).

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

produce, and disseminate foreign intelligence information.” 50 U.S.C. §§ 1801(h), 1821(4)(A). As explained by the Foreign Intelligence Surveillance Court of Review, “By minimizing acquisition, Congress envisioned that, for example, where a switchboard line is tapped but only one person in the organization is the target, the interception should probably be discontinued where the target is not a party to the communication. By minimizing retention, Congress intended that information acquired, which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible. Furthermore, even with respect to information needed for an approved purpose, dissemination should be restricted to those officials with a need for such information.” In re Sealed Case, 310 F.3d 717, 731 (Foreign Int. Surv. Ct. Rev. 2002) (internal quotation marks omitted) (emphasis in original). But, 50 U.S.C. § 1801(h)(3) expressly states that the government is not required to minimize information that is “evidence of a crime.”

“Although FISA is chiefly directed to obtaining ‘foreign intelligence information,’ the Act specifically contemplates cooperation between federal authorities collecting [FISA material] and federal law enforcement officers” and “explicitly allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions.” Rosen, 447 F. Supp. 2d at 544. If the government intends to use FISA evidence in the criminal trial of an “aggrieved person,” it must notify the aggrieved person and the court of this intent. 50 U.S.C. §§ 1806(c), 1825(d). An aggrieved person “may move to suppress the evidence obtained or derived from such 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.” 50 U.S.C. §§ 1806(e), 1825(f). Upon such a motion, “if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States,” the

district court “shall” review the relevant FISA materials in camera and ex parte “to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” 50 U.S.C. §§ 1806(f), 1825(g). The court may disclose the FISA materials or portions thereof to the aggrieved person, “only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” 50 U.S.C. § 1806(f); see also 50 U.S.C. § 1825(g).

In the Fourth Circuit, the district court’s review of FISA materials is de novo, Squillacote, 221 F.3d at 554, and, given that “review is ex parte and thus unaided by the adversarial process,” the review should be both “searching and conducted with special care.” Rosen, 447 F. Supp. 2d at 545. But, just as the FISC applies a “clearly erroneous” standard to the specification, 50 U.S.C. §§ 1805(a)(4), 1824(a)(4), at the district court, the FISA application carries a “strong presumption of veracity and regularity,” United States v. Hassan, 742 F.3d 104, 139 (4th Cir. 2014). As with probable cause to believe that criminal activity is occurring, probable cause to believe that the target of FISA surveillance is an agent of a foreign power “is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” Hammoud, 381 F.3d at 332 (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983)). In evaluating probable cause, a judge must “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability’ that the search will be fruitful.” Id. (quoting Gates, 462 U.S. at 238). Stated differently, “[p]robable cause means more than bare suspicion but less than absolute certainty that a search will be fruitful.” Id. (quoting Mason v. Godinez, 47 F.3d 852, 855 (7th Cir. 1995)).

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

II. DISCUSSION

As a threshold matter, defense counsel contends that he needs access to the FISA material to develop suppression arguments. Def. Mem. at 8. This argument is unpersuasive. FISA expressly states that a court “shall” review FISA materials ex parte and in camera “if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.” 50 U.S.C. §§ 1806(f), 1825(g).⁷ The Attorney General has submitted such an affidavit, [Dkt. No. 82], and it is not for the Court to second guess his determination that disclosure of the FISA materials would be harmful to national security. Cf. C.I.A. v. Sims, 471 U.S. 159, 180 (1985) (“[I]t is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency’s intelligence-gathering process.”). FISA’s ex parte and in camera review procedures are not, as defendant claims, “incompatible with the adversary system that is the keystone of Anglo-American criminal justice.” Def. Mem. at 12. To the contrary, they are congressionally authorized and their constitutionality has been affirmed by the Fourth Circuit, United States v. Pelton, 835 F.2d 1067, 1075–76 (4th Cir. 1987) (“We find the provisions of

⁷ Defendant misquotes the statute as stating that “a review in camera and ex parte [of] the application, order, and such materials relating to the surveillance [] may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” Def. Mem. at 9 (alterations in original). This mutilation of the statute grossly misrepresents its meaning. Accurately quoted, the statute contains a mandatory, rather than a permissive instruction: “the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” 50 U.S.C. § 1806(f) (emphasis added); see also 50 U.S.C. § 1825(g).

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

FISA to be 'reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens,' and therefore compatible with the Fourth Amendment." (citing United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 323 (1972)), as well as every other federal court that has considered the matter, Gov. Opp. at 20-21 (collecting cases).

In addition, the exception to the requirement of ex parte, in camera review applies "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f), 1825(g). "[S]uch disclosure is 'necessary' only where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701, at 64 (1978)). Reviewing ex parte applications to determine if they establish probable cause is a traditional function of courts and, unsurprisingly, no court in the Fourth Circuit or elsewhere has concluded that defense input was necessary to determine the legality of FISA materials. Gov. Opp. at 17. This case is no exception. Having reviewed the FISA application(s), order(s), and other materials, the Court finds that they contain no facial inconsistencies, ambiguities, or inaccuracies and disclosure is not necessary to make an accurate determination of the legality of the surveillance.

Defendant also attacks the legality of the FISA application(s), arguing that based on its ex parte and in camera review the Court should suppress all the FISA evidence because "there is no

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

conceivable set of facts that would satisfy” the FISA requirements. Def. Mem. at 15. This necessarily speculative contention is based on defendant’s claim that he never had any interactions with a “foreign power,” Def. Mem. at 16-17, has never been the “agent” of a foreign power, *id.* at 17-18, and has never engaged in “international terrorism,” *id.* at 18-19. In addition, defendant argues that there was never any basis for searching his phone, text messages, email, Facebook, and property. *Id.* at 19-21. These arguments, which assume that the defendant was the target of the FISA application(s), are essentially an attack on probable cause. Without commenting on the target(s) of the FISA application(s), the Court finds that there was probable cause to believe that certain identified organization(s) were a “foreign power” within the meaning of 50 U.S.C. § 1801(a), which includes a “group engaged in international terrorism or activities in preparation therefor,” and that the target(s) knowingly acted for or on behalf of those organizations, or knowingly aided or abetted those organizations and were therefore “agent(s) of a foreign power” under 50 U.S.C. §§ 1801(b)(2), 1821(1).⁸ In addition, the application(s) establish probable cause to believe that each facility or place at which electronic surveillance was directed “[was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power” and the premises to be physically searched was, or was about to be, owned, used, possessed by, or was in transit to or from the target(s).

⁸ Defendant’s argument that he never “engaged in ‘international terrorism,’” Def. Mem. at 18, is misplaced as there is no such requirement in FISA. Instead the statute requires a certification that the information sought is “foreign intelligence information,” 50 U.S.C. § 1804(a)(6), which includes information that “relates to . . . international terrorism,” 50 U.S.C. § 1801(e)(1), and that the application establish probable cause that the target is an agent of a “foreign power,” which includes a “group engaged in international terrorism,” 50 U.S.C. § 1801(a)(4). Although the Court will not comment on the identity of the target(s) or the foreign agent(s), the FISA application(s) satisfied both of those requirements.

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

Defendant's next argument is that the FISA application(s) were "likely improperly predicated on protected First Amendment activities." Def. Mem. at 21. This argument, which again assumes that the defendant was the target, is supported by neither facts nor law. FISA provides that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). The critical word in that provision is "solely." As the Rosen opinion made clear, as a statutory matter, "[f]rom this plain language, it follows that the probable cause determination may rely in part on activities protected by the First Amendment, provided the determination also relies on activities not protected by the First Amendment." 447 F. Supp. 2d at 548.⁹ From a constitutional perspective, just as it is entirely consistent with the First Amendment to make "evidentiary use of speech to establish the elements of a crime or to prove motive or intent" during a criminal proceeding, Wisconsin v. Mitchell, 508 U.S. 476, 489 (1993); see also United States v. Hassan, 742 F.3d 104, 127–28 (4th Cir. 2014) ("[T]he First Amendment was no bar to the government's use of the appellants' speech to demonstrate their participation in the charged conspiracies."), so too is it appropriate to use speech to establish probable cause to believe that a target of FISA surveillance is an agent of a foreign power. Therefore, even if defendant were a/the target, it would have been permissible for the FISA application to reference First Amendment protected activities, provided that there was other evidence of prohibited activity.

⁹ FISA's legislative history explains that "[t]he Bill is not intended to authorize electronic surveillance when a United States person's activities, even though secret and conducted for a foreign power, consist entirely of lawful acts such as lobbying or the use of confidential contacts to influence public officials, directly or indirectly, through the dissemination of information." S. Rep. No. 95–701 at 29.

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

Defendant also contends that “normal investigative techniques” could have been employed. Def. Mem. at 21. According to the statute, a FISA application must contain a certification that the information sought “cannot reasonably be obtained by normal investigative techniques.” 50 U.S.C. §§ 1804(a)(6)(C), 1826(a)(6)(C). Defendant’s argument regarding this provision again simply denies that there was a “‘foreign intelligence’ dimension” to his activities and urges the Court to “closely scrutinize the factual basis for any certification that ‘normal investigative techniques’ could not have been used in this case.” Def. Mem. at 21-22. The Court has done just that and finds that the certification(s) that the information sought could not reasonably have been obtained by normal investigative techniques was/were not clearly erroneous on the basis of the facts submitted.

Finally, defendant states that “[t]he [r]equired [m]inimization [p]rocedures [m]ay [n]ot [h]ave [b]een [f]ollowed.” Def. Mem. at 22. But, other than citing the legal basis for the minimization requirement and explaining why minimization is important, he provides no basis for this argument. Instead he simply states, “[i]f proper minimization procedures were not followed, the Court should suppress the FISA [e]vidence.” *Id.* This argument also fails. As the legislative history makes clear, “[a]bsent a charge that the minimization procedures have been disregarded completely, the test of compliance is whether a good faith effort to minimize was attempted.” *Rosen*, 447 F. Supp. 2d at 551 (citing S. Rep. No. 95-701 at 39). This is because, “[i]n enacting FISA, Congress recognized that ‘no electronic surveillance can be so conducted that innocent conversations can be totally eliminated.’” *Hammoud*, 381 F.3d at 334 (quoting S. Rep. No. 95-701 at 39). In addition, as courts recognize, “it is not always immediately clear into which category a particular conversation falls. A conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE

in code.” *Id.* Here, the Court finds that the FISA application(s) incorporated the appropriate minimization procedures, the order(s) issued by the FISC directed the government to comply with the appropriate minimization procedures, and the FISA-authorized surveillance and physical search abided by these procedures when applicable and otherwise demonstrated a “good faith effort to minimize the acquisition and retention of irrelevant information.” *Id.*

In sum, the Court finds that based on its *de novo* review of the FISA materials and FISC order(s) that the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted in compliance with FISA.¹⁰

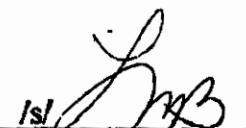
III. CONCLUSION

For these reasons, defendant’s Motion for Disclosure of FISA-Related Material and/or to Suppress the Fruits or Derivatives of Electronic Surveillance and Physical Search Pursuant to FISA [Dkt. No. 65] will be denied by an appropriate Order to be issued with this Memorandum Opinion.

The Clerk is directed to forward a copy of this Memorandum Opinion to counsel of record and CISO Maura Peterson.

Entered this 9th day of May, 2017.

Alexandria, Virginia



Leonie M. Brinkema
United States District Judge

¹⁰ Because the Court finds that the FISA application(s) at issue were supported by probable cause, it does not address the government’s argument regarding the good faith exception to the exclusionary rule, Gov. Opp. at 25-28, which presents a question that has not yet been addressed by the Fourth Circuit.

UNCLASSIFIED / CLEARED FOR PUBLIC RELEASE