UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	Criminal No.: 13-274 (RC)
	:	
v.	:	
	:	
SHANTIA HASSANSHAHI,	:	
	:	
Defendant.	:	
	:	

THE UNITED STATES' RESPONSE TO
DEFENDANT'S BRIEF RE EFFECT OF *ACLU V. CLAPPER*

On December 1, 2014, this Court denied Hassanshahi's motion to suppress highly incriminating evidence obtained by the government through a search of his computer, finding that, even assuming arguendo that the government somehow violated his constitutional rights by obtaining his phone number through the search of a government database, the search was a valid border search sufficiently attenuated from any alleged initial illegality by extensive additional investigation. *United States v. Hassanshahi*, __ F. Supp. 3d __, 2014 WL 6735479 (D.D.C. Dec. 1, 2014). As part of his months-long effort to seek reconsideration of this Court's decision, Hassanshahi now grasps at the Second Circuit's decision in *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), which arises out of a civil lawsuit challenging a counterterrorism telephony metadata collection program that is unrelated to the Drug Enforcement Administration ("DEA") database that was queried in this investigation. The panel in *Clapper* expressly declined to opine on the statutory basis for the DEA program, 785 F.3d at 812 n.6; the *Clapper* court's statutory analysis of the NSA program did not take account of the subsequently enacted USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268; and the Foreign Intelligence Surveillance Court ("FISC") recently found that the *Clapper* decision was erroneous based, in part, on the Second

Circuit's misunderstanding of how the anti-terrorism telephony metadata program actually operates, *see In re Application of the FBI for an Order Requiring the Production of Tangible Things*, BR 15-75, at 2 (F.I.S.C. June 29, 2015) (Mosman, J.) ("*In re Application V*") (attached as Exhibit A). Moreover, as explained below, nothing in the *Clapper* decision provides any basis for this Court to overturn its earlier decision denying Hassanshahi's motion to suppress.

To the extent that Hassanshahi seeks to transform his failed motion to suppress into a statutory challenge to the Drug Enforcement Administration's ("DEA") now discontinued program to collect certain telephony metadata, that effort fails both because (1) a criminal defendant may not challenge the statutory validity of a subpoena issued to a third party, and (2) the issuance of a subpoena beyond statutory authorization, even if it occurred, would not lead to a suppression remedy. The *Clapper* panel, writing in a civil case where plaintiffs sought injunctive relief (which was not granted), had no occasion to, and did not, opine on these barriers that prevent a criminal defendant, such Hassanshahi, from suppressing evidence based on an alleged lack of statutory authority.

BACKGROUND

I. The NSA's Telephony Metadata Program

The Second Circuit's *Clapper* decision arises out of a civil challenge to a counterterrorism telephony metadata program maintained by the National Security Agency ("NSA"). As the government has repeatedly informed the defendant (and the Court), that program was not used in this case. The NSA program involves the collection of telephony metadata pertaining to both domestic and international telephone calls pursuant to court orders

issued by the Foreign Intelligence Surveillance Court ("FISC").[1] The FISC issues these orders pursuant to 50 U.S.C. § 1861(c), which is Section 501 of the Foreign Intelligence Surveillance Act ("FISA"), as amended, and which is also known as "Section 215" because Section 501 was amended by Section 215 of the USA PATRIOT Act. The government's applications for orders pursuant to this provision must contain, *inter alia*, "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized [terrorism] investigation (other than a threat assessment)." 50 U.S.C. § 1861(b)(2)(A).

The telephony metadata collected under the NSA program includes "'comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, [equipment identity numbers], etc.), trunk identifier, telephone calling card numbers, and time and duration of call.'" *Clapper*, 785 F.3d at 797 (quoting a FISC order issued to a telephone services provider). The Second Circuit appeared to accept the *Clapper* plaintiffs' assertion that the NSA program collects "virtually all telephony metadata associated with calls made or received in the United States," although the government disputes this characterization.[2] *Id.* As of the time the *Clapper* decision was issued, the program

[1] As this Court is likely aware, the FISC is an Article III court comprised of U.S. District Court judges from around the country. *See* 50 U.S.C. § 1803(a); *United States v. Cavanagh*, 807 F.2d 787, 791-92 (9th Cir. 1987) (Kennedy, J.); *United States v. Megahey*, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982). Its decisions are subject to review in the Foreign Intelligence Court of Review, which is comprised of U.S. Court of Appeals judges, and ultimately in the U.S. Supreme Court. *See*, *e.g.*, 50 U.S.C. §§ 1803(b), 1861(f)(3). The FISC is not, as Hassanshahi baselessly asserts, "a Star Chamber." Def.'s Br. Re Effect of *ACLU v. Clapper*, ECF No. 68, at 7 ("Def.'s Br.").

[2] The precise scope of the NSA program was (and remains) classified, and thus the government was not able to provide specific facts to rebut the plaintiffs' characterization.

had been approved approximately three dozen times by at least 15 different district court judges sitting on the FISC.[3]

Over the last two years, the NSA program has been challenged in several cases. The primary arguments that have been advanced are that the program violates the Fourth Amendment and that the program exceeds statutory authorization. The former argument has been accepted by Judge Leon of this Court, but rejected by every other court to address it on the grounds that it is precluded by the third-party doctrine set forth in a series of Supreme Court and lower court opinions, such as *Smith v. Maryland*, 442 U.S. 735 (1979).[4] The statutory argument, in addition to being inconsistent with numerous FISC decisions, was rejected by the two district courts to address it. Judge Leon found that the statutory question was committed by Congress to the FISC

[3] *See, e.g.*, *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, 2013 WL 5741573 (F.I.S.C. Aug. 29, 2013) (Eagan, J.) ("*In re Application I*"); *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR 13-158 (F.I.S.C. Oct. 11, 2013) (McLaughlin, J.) ("*In re Application II*"), available at www.fisc.uscourts.gov/sites/default/files/BR%2013-158%20Memorandum-1.pdf; *In Re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR 14-96 (F.I.S.C. June 19, 2014) (Zagel, J.) ("*In re Application IV*"), available at www.fisc.uscourts.gov/sites/default/files/BR% 2014-96%20Opinion-1.pdf.

[4] *Compare Klayman v. Obama*, 957 F. Supp. 2d 1, 37 (D.D.C. 2013) ("I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star [*Smith v. Maryland*,] a case that predates the rise of cell phones") *with Smith v. Obama*, 24 F. Supp. 3d 1005, 1010 (D. Idaho 2014) ("*Smith* [*v. Maryland*] was not overruled, and it continues . . . to bind this Court. This authority constrains the Court from joining *Klayman*."), *ACLU v. Clapper*, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013) (Call "records are created and maintained by the telecommunications provider, not the [caller]. Under the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information.") (citing *Smith*), *rev'd on other grounds*, 785 F.3d 787 (2d Cir. 2015), *and United States v. Moalin*, 2013 WL 6079518, at *7 (S.D. Cal. Nov. 18, 2013) ("Here, when Defendant Moalin used his telephone to communicate with third parties, whether in Somalia or the United States, he had no legitimate expectation of privacy in the telephone numbers dialed."); *see also In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things*, Dkt. No. BR 14-01, at 9 (F.I.S.C. Mar. 20, 2014) (Collyer, J.) ("*In re Application III*") (finding "Judge Leon's analysis in *Klayman* to be unpersuasive"), available at www.fisc.uscourts.gov/sites/default/files/BR%2014-01%20Opinion%20and%20Order-1.pdf.

and not to the district courts, *Klayman v. Obama*, 957 F. Supp. 2d 1, 20-23 (D.D.C. 2013), a ruling that (unlike that opinion's Fourth Amendment holding) has not been appealed. Judge Leon observed that permitting "broader judicial review than that specifically set forth" in FISA would require "[j]udicial alchemy" of a "sort [that] is particularly inappropriate [in] matters affecting national security." *Id.* at 22-23. The district court in *Clapper* evinced a similar respect for the FISC's role and expertise. *ACLU v. Clapper*, 959 F. Supp. 2d 724, 738-42 (S.D.N.Y. 2013), *rev'd*, 785 F.3d 787 (2d Cir. 2015). Alternatively, the *Clapper* district court held that the NSA program was fully authorized by 50 U.S.C. § 1861. *See* 959 F. Supp. 2d at 746-49.

On appeal, a panel of the Second Circuit disagreed with the district court on both of these statutory points. The panel first found that, notwithstanding the apparent statutory commitment of the issue to the FISC, it could review the question of whether the NSA program was authorized by 50 U.S.C. § 1861, relying in part on "the doctrine of constitutional avoidance." *Clapper*, 785 F.3d at 808. The panel then found that the NSA program was not statutorily authorized, finding that the approach repeatedly approved by the FISC "essentially reads the 'authorized investigation' language out of the statute," *id.* at 815-16, and is inconsistent with the "(other than a threat assessment)" language in Section 1861. 785 F.3d at 816-17. Despite finding that the NSA program exceeded statutory authorization, the panel declined to "conclude that a preliminary injunction is required," reasoning that Congress should be given time to consider whether to authorize continued use of the NSA program. *Id.* at 826; *see also id.* at 824 ("Congress is better positioned than the courts to understand and balance the intricacies and competing concerns involved in protecting our national security, and to pass judgment on the value of the telephone metadata program as a counterterrorism tool.").

On June 1, 2015, the statutory provision underlying the NSA program (Section 215 of the USA PATRIOT Act, which amended 50 U.S.C. § 1861) expired. *See In re Application V*, at 2. On June 2, 2015, Congress enacted the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, which "effectively restored the version of [50 U.S.C. § 1861] that had been in effect [prior to] the June 1 sunset." *In re Application V*, at 9.[5] Also on June 2, the government applied to the FISC for an order allowing the NSA program to restart. *Id.* at 3. On June 9, 2015, citing the USA FREEDOM Act, the Second Circuit, *sua sponte*, stayed the issuance of its mandate and ordered supplemental briefing by July 24, 2015. Order, *ACLU v. Clapper*, No. 14-42 (2d Cir. June 9, 2015), ECF No. 190.

On June 29, 2015, after considering submissions from the government and two *amici curiae* (who argued that the NSA program was unlawful), the FISC granted the government's application. *See In re Application V*, at 1. In finding that the NSA program was indeed authorized by 50 U.S.C. § 1861, the FISC stated that it "respectfully disagree[d] with [the Second Circuit's] analysis," in *Clapper*. *Id.* at 15. The FISC further explained that "the Second Circuit's analysis rests on mischaracterizations of how [the NSA] program works" and that the Second Circuit's "description [of the program] bears little resemblance to how the government actually uses the records." *Id.* at 16.

II. The DEA's Telephony Metadata Program

The DEA's now-discontinued practice of obtaining telephony metadata in connection with its broad authority to investigate narcotics crimes was significantly different from the NSA program at issue in *Clapper*. Under the DEA program, the DEA submitted administrative

[5] The USA FREEDOM Act contains a restriction on the use of 50 U.S.C. § 1861 for bulk collection and enacts an alternative program for acquiring telephony metadata, but those provisions do not go into effect until November 29, 2015. *See In re Application V*, at 10.

subpoenas to certain U.S. telecommunications service providers. Exhibit B, ¶ 2.[6] These subpoenas were based on the DEA's administrative subpoena power provided by 21 U.S.C. § 876, *see* Exhibit B, ¶ 2, which gives "the DEA broad powers to investigate," *United States v. Moffett*, 84 F.3d 1291, 1293 (10th Cir. 1996), by permitting the subpoena of records that the Attorney General or her designee "finds relevant or material to [an] investigation" concerning "controlled substances, listed chemicals, tableting machines, or encapsulating machines," 21 U.S.C. § 876(a).

The DEA subpoenas sought metadata relating only to international telephone calls that originated in the United States and terminated in certain designated foreign countries that were determined to have a demonstrated nexus to international drug trafficking and related criminal activities.[7] Exhibit B, ¶ 2. This metadata consisted exclusively of the initiating telephone number; the receiving telephone number; the date, time, and duration of the call; and the method by which the call was billed. *Id.* The metadata was stored in a separate database in the sole possession of the DEA. *Id.* This database did not include any subscriber information, other personal identifying information, or communication content. *Id.* In September 2013, the DEA program was suspended, the data collection at issue ceased, the existing data was quarantined, and no further queries of the data were made. *Id.* ¶ 3. The program was ultimately terminated, and the database was purged of the collected data. *Id.*

[6] Exhibit B is a declaration recently filed on behalf of the DEA in *Human Rights Watch v. DEA*, 2:15-cv-2573 (C.D. Cal.), a case civil in which the plaintiff has challenged the DEA's former program. The declarant, Robert W. Patterson, submitted a similar declaration in this case. *See* ECF No. 49-1.

[7] Hassanshahi is thus incorrect when he asserts that the DEA program collected information on "all telephone calls to or from abroad." Def.'s Br., ECF No. 68, at 2. The program collected only records related to international calls *from* the United States (not to the U.S.), and only calls to some (not all) foreign countries.

While the information was collected for use in the DEA's narcotics-related investigatory work, in some instances the DEA shared limited information with other law enforcement agencies to assist in non-narcotics federal criminal investigations. *Id.* ¶ 2. On August 24, 2011, the DEA, at the request of Homeland Security Investigations, queried an Iranian number based on a reasonable articulable suspicion that the Iranian number was being used for the purpose of importing technological goods to Iran in violation of U.S. law. *Id.* DEA then provided HSI with a single telephone detail record that showed a call from a U.S. number, which turned out to be Hassanshahi's, to the suspect Iranian number. *See* Opp'n to Def.'s Mot. to Suppress Evidence, ECF No. 37, at 2. After extensive additional investigation, HSI developed evidence that Hassanshahi had violated U.S. law, and this prosecution resulted. *See id.* at 2-5.

Contrary to Hassanshahi's assertion, Def's Br., ECF No. 68, at 11, at the time it issued the *Clapper* decision, the Second Circuit was fully aware of the DEA program. *See Clapper*, 785 F.3d at 812 n.6 (noting the "recently disclosed, now discontinued program under which the Drug Enforcement Administration utilized administrative subpoenas obtained pursuant to 21 U.S.C. § 876 to collect and maintain a telephone metadata database"). The Second Circuit made clear that it was not considering or ruling on the statutory authority for the DEA program: "That program, which, according to both parties, has been discontinued, is not being challenged here, and we therefore need not opine as to whether the language of the statute pursuant to which the metadata were collected [*i.e.*, Section 876] authorized that program." *Id.*

ARGUMENT

Defendant's rhetoric aside, the Second Circuit's *Clapper* decision provides no basis for this court to reconsider, much less reverse, its earlier decision denying Hassanshahi's motion to suppress. The *Clapper* panel, in a civil case that did not involve the DEA subpoena authority at all, had no occasion to consider (1) whether a defendant in a criminal prosecution may challenge a subpoena issued to a third party on the grounds that the subpoena allegedly exceeded statutory authority; and (2) whether there is a suppression remedy for the issuance of a subpoena in alleged excess of statutory authority. As demonstrated in the government's previous filings, the defendant may not maintain such a challenge, and, in any event, any such challenge could not lead to suppression.

I. The Second Circuit's Standing Analysis in *Clapper*, a Civil Case, Has No Relevance to the Issues Presented in this Criminal Prosecution

Hassanshahi's discussion of *Clapper*'s standing analysis conflates two entirely different concepts—the Article III standing of plaintiffs to bring a civil case and a criminal defendant's prudential standing to challenge the means by which the government obtained evidence against him. These are simply different legal doctrines, and the Second Circuit's analysis of the former does not assist Hassanshahi as to the latter.

In order to establish Article III standing to bring a civil claim, a plaintiff must demonstrate (1) a concrete and particularized injury, (2) that was caused by the defendant's allegedly unlawful action, and (3) is judicially redressable. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). In *Clapper*, the government argued that the plaintiffs failed to satisfy the first prong of this test because any injury they alleged was not "sufficiently concrete or imminent to confer standing." *Clapper*, 785 F.3d at 800. The Second Circuit disagreed, finding that the plaintiffs had "standing to allege injury from the collection, and maintenance in a

government database, of records relating to them." *Id.* at 801; *see also id.* at 802 (finding that the electronic search of a database containing records relating to plaintiffs was a sufficient injury to support standing).

Hassanshahi's inability to challenge the validity of the subpoena that led to the government acquiring a call detail record of a call from his phone number to an Iranian phone number does not relate to whether he has a concrete or particularized injury. Rather, it is an application of the principle that "the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant." *United States v. Miller*, 425 U.S. 435, 444 (1976). Hassanshahi's deficiency is not that he lacks injury; it is that he lacks any legal right to challenge the statutory validity of an administrative subpoena issued to someone else. *E.g.*, *United States v. Plunk*, 153 F.3d 1011, 1020 (9th Cir.) (holding that a criminal defendant could not challenge legality of third party subpoena issue pursuant to 21 U.S.C. § 876(a) to obtain records of defendant's phone calls), *amended on other grounds*, 161 F.3d 1195 (9th Cir. 1998); *United States v. Moffett*, 84 F.3d 1291, 1293-94 (10th Cir. 1996) (holding that a criminal defendant could not challenge legality of third party subpoena issue pursuant to 21 U.S.C. § 876(a) because non-recipients are not within "the zone of interest" protected by that statute); *United States v. Phibbs*, 999 F.2d 1053, 1076-78 (6th Cir. 1993) (holding that a criminal defendant could not challenge legality of third party subpoenas issue pursuant to 21 U.S.C. § 876(a) to obtain records of defendant's phone calls and credit card transactions); *see also United States v. Kember*, 648 F.2d 1354, 1365 (D.C. Cir. 1980) ("[T]he Supreme Court has made clear in recent years that a defendant has no standing to object to the introduction of evidence illegally seized from a third party."). The Second Circuit's discussion of Article III standing requirements in a civil case has no bearing on the longstanding legal doctrine that bars

Hassanshahi's challenge, namely that a criminal defendant cannot challenge the statutory validity of a subpoena that was not issued to him.

II. The *Clapper* Decision Provides No Basis for Suppression in this Case

It is undisputed that there is ordinarily no suppression remedy for a statutory violation. *See* Response to Court's Directive, ECF No. 51, at 6-9. Hassanshahi claims that this case is different because there are "sufficient 4th amendment implications." Def.'s Br., ECF No. 68, at 13. As the government explained in its response to Hassanshahi's last filing making this claim, this is incorrect. *See* Reply to Def.'s Resp., ECF No. 58, at 2-3; *see also id.* at 3-6 (explaining that the government has not conceded, and in fact strongly disputes, the existence of any Fourth Amendment violation in this case). *Clapper*, moreover, does not assist Hassanshahi's argument.

In *Clapper*, the Second Circuit expressly declined to reach the plaintiffs' contention that the NSA program violated the Fourth Amendment. 785 F.3d at 792. Every court but one that has actually reached this issue has found that the NSA program does not violate the Fourth Amendment due to the third-party doctrine set forth in cases such as *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), *United States v. Miller*, 425 U.S. 435 (1976), and *California v. Greenwood*, 486 U.S. 35 (1988). *See supra*, at 4 & n.4. Pursuant to that doctrine, "telephone numbers [obtained via call records] are not protected by the Fourth Amendment." *United States v. Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000) (citing *Smith v. Maryland*). Only the Supreme Court could reconsider or amend the third-party doctrine, *see Agostini v. Felton*, 521 U.S. 203, 237 (1997), and it has not done so. *See, e.g.*, *United States v. Davis*, 785 F.3d 498, 511-15 (11th Cir. 2015) (en banc); *United States v. Wheelock*, 772 F.3d 825, 829 (8th Cir. 2014); *In re Application of the United States*, 724 F.3d 600, 608-15 (5th Cir. 2013).

Moreover, the call detail record at issue in this case, a record of a single *international* call, is not subject to constitutional protection for an additional reason, given that the government can, without individualized suspicion and consistent with the Fourth Amendment, open international letters to inspect their contents. *See United States v. Ramsey*, 431 U.S. 606, 607-08 (1977). Thus, Hassanshahi could have had no reasonable expectation that the government would not obtain, from a telephone provider, a mere call record of a call from his number to a procurer in Iran. *See Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (holding that a person claiming Fourth Amendment protection "must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable").

Finally, as this Court has specifically held, even if there were an underlying Fourth Amendment violation in the DEA's acquisition of a call detail record concerning Hassanshahi's call to Iran, suppression would not be warranted because of the attenuation doctrine. *Hassanshahi*, 2014 WL 6735479. The fact that a panel of the Second Circuit, counter to every other federal judge to have adjudicated the issue, found that a different telephony metadata program maintained by a different agency was not authorized by a different statute provides no basis for this Court to reconsider its earlier ruling denying Hassanshahi's motion to suppress.

Conclusion

For the reasons stated above and in the government's previous filings, *see* ECF Nos. 51, 58, there is no basis to revisit this Court's decision to deny Defendant's motion to suppress.

July 10, 2015

Respectfully submitted,

VINCENT H. COHEN, Jr.
Acting United States Attorney

FREDERICK YETTE, D.C. Bar 385391
Assistant United States Attorney
National Security Section
555 4th Street, N.W.
Washington, D.C. 20530

/s/ Jeffrey M. Smith
JEFFREY M. SMITH, D.C. Bar 467936
Appellate Unit
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530