UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	
	:	Criminal Action No.: 13-0274 (RC)
SHANTIA HASSANSHAHI,	:	
also known as Shantia Hassan Shahi,	:	
also known as Shahi,	:	
also known as Shantia Haas,	:	
also known as Sean Haas,	:	
	:	
and	:	
	:	
HASSTON, INC.,	:	
	:	
Defendants.	:	

MEMORANDUM & ORDER

DENYING DEFENDANT'S MOTION FOR RECONSIDERATION

I. INTRODUCTION

Defendant Shantia Hassanshahi is charged with one count of conspiracy to violate the International Economic Emergency Powers Act, 50 U.S.C. § 1705, and the Iranian Transactions and Sanctions Regulations, 31 C.F.R. §§ 560.203–204, commonly referred to as the United States' trade embargo against Iran.

In December 2014, the Court denied a motion by Mr. Hassanshahi to suppress certain evidence discovered during a forensic examination of his laptop computer, holding, in relevant part, that discovery of the evidence was sufficiently attenuated from a search of a mysterious telephony database that the Court assumed, for purposes of its analysis and at the Government's suggestion, was unconstitutional. *See United States v. Hassanshahi*, 75 F. Supp. 3d 101 (D.D.C. 2014). Following the Court's decision, Mr. Hassanshahi has argued, both orally before the Court

and in rounds of supplemental briefing in response to orders of the Court, that suppression of the evidence is warranted in light of both additional information concerning the database that the Government provided after the Court's ruling and the Second Circuit's recent decision concerning a different government database in *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).

The Court construes these arguments as a motion for reconsideration of the Court's denial of Mr. Hassanshahi's motion to suppress. For the reasons that follow, and upon consideration of the briefs submitted by both Mr. Hassanshahi and the Government, the Court denies that motion and affirms its ruling on the motion to suppress.

II. BACKGROUND

The Indictment against Mr. Hassanshahi alleges that, beginning in or around March 2009, Mr. Hassanshahi engaged in a conspiracy to export or cause the exportation of goods and technology from Canada to Iran, as well as related services from the United States to Iran, without first having obtained a license from the Office of Foreign Assets Control, in violation of federal law. *See* Indictment ¶ 1, ECF No. 7.

At trial, the Government seeks to introduce evidence discovered during a forensic examination of Mr. Hassanshahi's laptop computer, which the Government seized from Mr. Hassanshahi in January 2012 upon his arrival from the United States at the Los Angeles International Airport ("LAX"). The Government's search and seizure of that evidence was the result of an investigation that began at least as early as August 2011.[1] *See Hassanshahi*, 75 F.

[1] The Court described the investigation that led to the search and seizure of Mr. Hassanshahi's laptop computer in greater detail than is provided here in its memorandum opinion denying Mr. Hassanshahi's prior motion to suppress the evidence. The Court incorporates that factual background here by reference. *See Hassanshahi*, 75 F. Supp. 3d at 105–07.

Supp. 3d at 105–07. In August 2011, Homeland Security Investigations ("HSI") received an unsolicited e-mail from a source concerning an Iranian individual named "Sheikhi" who was seeking to procure protection relays for an Iranian power project. *See id.* at 105. Later the same month, HSI requested a search of a law enforcement database using a telephone number it knew to be associated with Sheikhi. That search returned a single telephone record of one call between the searched telephone number and a California telephone number with an 818 area code that HSI later determined, through its subsequent investigation, was registered to Mr. Hassanshahi. *See id.* at 105–06. Over the course of the next several months, HSI investigated Mr. Hassanshahi, which ultimately led to the search and seizure of his laptop computer at LAX.

Mr. Hassanshahi moved to suppress the evidence discovered through the forensic examination of his laptop, asserting, in relevant part, that HSI's search of the law enforcement database constituted an unconstitutional search and that the evidence should be excluded under the fruit of the poisonous tree doctrine. *See* Def.'s Mot. Suppress at 18–30, ECF No. 28. The Court denied Mr. Hassanshahi's motion, holding, in relevant part, that the exclusionary rule did not require suppressing the evidence as "fruit of the poisonous tree," because discovery of the evidence was sufficiently attenuated from the purportedly unlawful search of the database.[2] *See Hassanshahi*, 75 F. Supp. 3d at 108–18. The Court reached this holding based on limited information concerning the database at issue, because, in its opposition to the motion to suppress, the Government refused to provide details concerning the database and instead asked the Court to assume *arguendo* that the database was unconstitutional. *See id.* at 109. In its analysis, the

[2] The Court also rejected Mr. Hassanshahi's separate argument that the evidence should be suppressed because the Government lacked reasonable suspicion to conduct the forensic examination of the laptop computer, holding that the Government had reasonable suspicion and declining to reach the constitutional issue of whether reasonable suspicion was required. *See Hassanshahi*, 75 F. Supp. 3d at 118–26. That holding is not at issue here.

Court therefore proceeded on the assumption that the database and HSI's search of the database were unconstitutional and nevertheless concluded that the exclusionary rule did not require suppression. *See id.* at 108–18. Although the Court was unequivocal in its holding, it also ordered the Government to provide the Court with more information concerning the database. *See id.* at 115 n.6.

The Government complied with the Court's order by providing a declaration from Robert Patterson, an Assistant Special Agent in Charge at the United States Drug Enforcement Administration ("DEA"), which the Government initially filed *ex parte* and under seal and later filed publicly in redacted form. *See* Decl. Robert Patterson ("Patterson Decl."), ECF No. 49-1 (publicly-filed redacted version). In this declaration, Mr. Patterson explained that the database at issue "consisted of telecommunications metadata obtained from United States telecommunications providers pursuant to administrative subpoenas served upon the service providers under the provisions of 21 U.S.C. § 876." *Id.* ¶ 4. The referenced statutory provision authorizes the Attorney General to issue administrative subpoenas in "any investigation" relating to his drug enforcement function. *See* 21 U.S.C. § 876. Mr. Patterson provided further detail concerning the metadata stored in the database:

> This metadata related to international telephone calls originating in the United States and calling [REDACTED] designated foreign countries, one of which was Iran, that were determined to have a demonstrated nexus to international drug trafficking and related criminal activities. 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. No subscriber information or other personal identifying information was included in this database. No communication content was included in this database.

Patterson Decl. ¶ 4. Mr. Patterson further stated that the DEA database "could be used to query a telephone number where federal law enforcement officials had a reasonable articulable suspicion

that the telephone number at issue was related to an ongoing federal criminal investigation" and that the standard had been met with respect to the search that returned Mr. Hassanshahi's telephone number. *Id.* ¶ 5. Mr. Patterson also stated that use of this particular database was suspended in September 2013 and that "information is no longer being collected in bulk pursuant to 21 U.S.C. § 876." *Id.* ¶ 6.

At a status conference before the Court on January 29, 2015 following the filing of Mr. Patterson's redacted declaration, counsel for Mr. Hassanshahi sought permission to renew his motion to suppress based on the new information concerning the DEA database. The Court directed the Government to provide briefing concerning two issues: first, whether information obtained by one law enforcement agency for one purpose may lawfully be shared with another law enforcement agency for another purpose; and second, whether a remedy of suppression existed for a non-constitutional violation of law. The Government submitted a brief on these issues, and Mr. Hassanshahi filed a brief in response, to which the Government filed a reply brief. *See* Gov't's Response to the Court's Directive from the Jan. 29, 2015 Status Conference ("Gov't's Feb. 25 Brief"), ECF No. 51; Def.'s Response to Gov't's Filing ("Def.'s Apr. 13 Brief"), ECF No. 53; Gov't's Reply to Def.'s Response ("Gov't's Apr. 29 Brief"), ECF No. 58.

In May 2015, the Second Circuit decided *ACLU v. Clapper*, holding that a counterterrorism telephony metadata program maintained by the National Security Agency ("NSA"), which this Court discussed in its denial of the motion to suppress, exceeded the program's statutory authorization. *See ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). The parties have also submitted briefs concerning the effect, if any, that the Second Circuit's decision might have on the issues presented in this case. *See* Def.'s Brief re Effect of *ACLU v. Clapper*

("Def.'s June 22 Brief"), ECF No. 68; Gov't's Response to Def.'s Brief ("Gov't's July 10 Brief"), ECF No. 74; Def.'s Reply ("Def.'s July 29 Brief"), ECF No. 77.

III. LEGAL STANDARD

"Although the Federal Rules do not specifically provide for motions for reconsideration in criminal cases, the Supreme Court has recognized, in *dicta*, the utility of such motions." *United States v. Ferguson*, 574 F. Supp. 2d 111, 113 (D.D.C. 2008); *see also United States v. Dieter*, 429 U.S. 6, 8 (1976) (per curiam) (noting "the wisdom of giving district courts the opportunity to promptly correct their own alleged errors"). Courts in this District have, therefore, entertained motions for reconsideration in criminal cases by importing the standards of review applicable in motions for reconsideration in civil cases. *See, e.g.*, *United States v. Trabelsi*, Crim. No. 06-89 (RWR), 2015 WL 5175882 at *2 (D.D.C. Sept. 3, 2015); *United States v. Slough*, 61 F. Supp. 3d 103, 107 (D.D.C. 2014); *United States v. Cabrera*, 699 F. Supp. 2d 35, 39 (D.D.C. 2010); *United States v. Sunia*, 643 F. Supp. 2d 51, 60–61 (D.D.C. 2009); *United States v. Libby*, 429 F. Supp. 2d 46, 46–47 (D.D.C. 2006). With respect to motions for reconsideration of final judgments, courts have adopted the standard of review for motions filed under Rule 59(e) of the Federal Rules of Civil Procedure. *See Slough*, 61 F. Supp. 3d at 107 n.1 (citing cases). With respect to interlocutory decisions, courts in this District have also adopted the standard from civil cases that reconsideration of an interlocutory decision is available "as justice requires." *See Trabelsi*, 2015 WL 5175882 at *2; *Slough*, 61 F. Supp. 3d at 107; *Sunia*, 643 F. Supp. 2d at 60–61.

The Court's denial of Mr. Hassanshahi's motion to suppress was an interlocutory decision, and, therefore, the Court follows the lead of other courts in this District and applies the "as justice requires" standard. "[A]sking 'what justice requires' amounts to determining, within

the Court's discretion, whether reconsideration is necessary under the relevant circumstances." *Cobell v. Norton*, 355 F. Supp. 2d 531, 539 (D.D.C. 2005). In making this determination, the Court considers whether it "patently misunderstood a party, has made a decision outside the adversarial issues presented to the Court by the parties, has made an error not of reasoning but of apprehension, or where a controlling or significant change in the law or facts [has occurred] since the submission of the issue to the Court." *Singh v. George Washington Univ.*, 383 F. Supp. 2d 99, 101 (D.D.C. 2005) (internal quotation and citation omitted).

The Court is also guided by several generally applicable principles. "'Motions for reconsideration are committed to the sound discretion of the trial court.'" *Trabelsi*, 2015 WL 5175882 at *2 (quoting *Judicial Watch, Inc. v. U.S. Dep't of Energy*, 319 F. Supp. 2d 32, 34 (D.D.C. 2004)). Also, "[t]he moving party bears the burden 'to show that reconsideration is appropriate and that harm or injustice would result if reconsideration were denied.'" *Id.* (quoting *United States v. Hemingway*, 930 F. Supp. 2d 11, 13 (D.D.C. 2013)). Moreover, a motion for reconsideration is "not simply an opportunity to reargue facts and theories upon which a court has already ruled." *New York v. United States*, 880 F. Supp. 37, 38 (D.D.C. 1995); *see also Singh*, 383 F. Supp. 2d at 101 ("[W]here litigants have once battled for the court's decision, they should neither be required, nor without good reason permitted, to battle for it again.").

IV. ANALYSIS

Mr. Hassanshahi and the Government advance a variety of arguments in connection with Mr. Hassanshahi's motion for reconsideration. These arguments can be grouped in two major issues for the Court to consider: first, whether Mr. Hassanshahi may seek suppression of the laptop evidence by challenging the statutory validity of the DEA database, as opposed to its constitutionality; and second, whether the new information disclosed by the Government

concerning the database and the Second Circuit's decision in *Clapper* require the Court to reverse its prior decision and suppress the evidence on constitutional grounds. The Court addresses these issues below.

A. Mr. Hassanshahi's Statutory Challenge

In his original motion to suppress the laptop evidence, Mr. Hassanshahi argued that the evidence should be suppressed on constitutional grounds. *See* Def.'s Mot. Suppress at 18–30. After the Court rejected that argument and denied the motion, the Government disclosed that the DEA obtained the information contained in the database from U.S. telecommunications service providers pursuant to administrative subpoenas that the Government asserts were authorized by 21 U.S.C. § 876. *See* Patterson Decl. ¶ 4. In light of this disclosure, Mr. Hassanshahi takes the position that the evidence should be suppressed not only on constitutional grounds, but also on statutory grounds, arguing that the DEA's collection and dissemination of the data violated 21 U.S.C. § 876. The Government takes the position, through several distinct arguments, that Mr. Hassanshahi is unable, as a matter of law, to challenge the statutory validity of the database and seek suppression of the evidence as a remedy. The Court addresses the Government's arguments in turn.

1. Mr. Hassanshahi's Ability To Raise A Statutory Challenge

The Government argues that Mr. Hassanshahi cannot challenge the statutory validity of the DEA database for two reasons. First, the Government argues that Mr. Hassanshahi cannot challenge the DEA's collection of the metadata contained in the database from telecommunications service providers, because he lacks "standing" to challenge administrative

subpoenas directed to third parties.[3] Second, the Government argues that Mr. Hassanshahi cannot challenge the DEA's dissemination of that information to HSI, because it is a longstanding rule that one law enforcement agency may share information it has collected for one purpose with another law enforcement agency for a different purpose.

With respect to the DEA's collection of the metadata, the Court observes that Mr. Hassanshahi is not the first criminal defendant to challenge an administrative subpoena issued to a third party under Section 876.[4] In *United States v. Moffett*, a case somewhat similar to this one, a criminal defendant challenged the Attorney General's authority to issue a subpoena to a third party under Section 876 purely on statutory grounds and sought to suppress the evidence gained through its use. *See United States v. Moffett*, 84 F.3d 1291, 1293 (10th Cir. 1996). The Tenth

---

[3] The Government uses the term "standing" throughout its briefs (occasionally using the term "prudential standing"), referencing the concept of "statutory standing," which is distinct from Article III standing. The Court eschews the terms "standing," "statutory standing," or "prudential standing" here, which the Supreme Court has acknowledged are "misleading." *Lexmark Int'l v. Static Control Components, Inc.*, 134 S. Ct. 1377, 1387 n.4 (2014). The D.C. Circuit has since clarified that "[s]tatutory standing is not really about standing at all, in the sense that it limits a 'court's constitutional power to adjudicate the case.' Instead, statutory standing is nothing more than an inquiry into whether the statute at issue conferred a 'cause of action' encompassing 'a particular plaintiff's claim.'" *United States v. Emor*, 785 F.3d 671, 677 (D.C. Cir. 2015) (quoting *Lexmark*, 134 S. Ct. at 1387).

[4] The Government also cites and relies upon some cases that addressed a criminal defendant's ability to challenge a subpoena directed at a third party on *constitutional* grounds. *See, e.g.*, *United States v. Miller*, 425 U.S. 435, 445 (1976) ("We hold that the District Court correctly denied respondent's motion to suppress, since he possessed no *Fourth Amendment* interest that could be indicated by a challenge to the subpoenas.") (emphasis added)); *United States v. Phibbs*, 999 F.2d 1053, 1077–78 (6th Cir. 1993) (holding that a defendant "did not have standing to dispute [the administrative subpoenas'] issuance *on Fourth Amendment grounds*") (emphasis added)). Whether Mr. Hassanshahi may bring a constitutional challenge to the DEA database is not at issue here, as the Court already assumed he could do so in its denial of the motion to suppress. The Government does not challenge that assumption. *See, e.g.*, Gov't's Apr. 29 Brief at 2 ("To the extent that a defendant asserts a violation of his own legal rights he has standing to do so. Hassanshahi did so in his original suppression motion, in which he claimed a violation of his Fourth Amendment rights. While defendant had standing to make this motion, it lacked merit, and it was denied.").

Circuit denied the defendant's attempted challenge, because it found that the defendant did not come within "the zone of interest the statute is meant to protect." *Id.* In its reasoning, the court observed that Section 876 "is written to give the DEA broad powers to investigate violations of federal drug laws" and that it "provides no express right to challenge the Attorney General's subpoenas issued under it." *Id.* The court contrasted another administrative subpoena statute, 26 U.S.C. § 7609, which provides a person whose records are subpoenaed from third parties by the Internal Revenue Service with a right to intervene and challenge the subpoena. *See id.* at 1293–94. The court also acknowledged analogous cases in which courts had similarly denied criminal defendants' challenges to the statutory validity of a search without adjudicating the merits of the claimed violation. *See id.* at 1294 (citing *United States v. Zermeno*, 66 F.3d 1058, 1062 (9th Cir. 1995)). At least one other circuit has followed *Moffett*, holding that a criminal defendant did not possess "statutory standing" to attack an administrative subpoena issued under Section 876 to a third party. *See United States v. Plunk*, 153 F.3d 1011, 1020 (9th Cir. 1998), *amended and reh'g denied* 161 F.3d 1195 (1998), *cert. denied* 526 U.S. 1060 (1999).

In his limited response, Mr. Hassanshahi points to *Clapper*, in which the Second Circuit held, in relevant part, that targets of orders issued pursuant to Section 215 of the PATRIOT Act could bring suit against the Government challenging the orders under the Administrative Procedure Act even though they were not the recipients of the orders.[5] *See Clapper*, 785 F.3d at

[5] Mr. Hassanshahi makes other arguments that are clearly without merit. He claims, for example, that the Government has "conceded" standing by also "conced[ing] that use of the database was a constitutional violation." Def.'s Apr. 13 Brief at 9–10. To be clear, the Government has never conceded that the DEA database was unconstitutional, nor has this Court held that it was. Rather, the Government asked the Court to assume, solely for purposes of the motion to suppress, that it was unconstitutional, which is what the Court did. *See Hassanshahi*, 75 F. Supp. 3d at 109. Moreover, Mr. Hassanshahi's argument conflates his standing to bring a *constitutional* challenge with his ability to bring a *statutory* challenge. As discussed, *supra* note 4, only the latter is at issue here. Mr. Hassanshahi also cites the Second Circuit's discussion of

803–10. Mr. Hassanshahi, however, neither references the Administrative Procedure Act nor explains how the Second Circuit's reasoning would apply in this case, in which, as a criminal defendant, he seeks to challenge the validity of a different program under an administrative subpoena statute.

With respect to the DEA's dissemination of the metadata to HSI, the Government argues that the DEA "acted consistently with the longstanding legal rule that '[e]vidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken.'" Gov't's Feb. 25 Brief at 4 (quoting *Jabara v. Webster*, 691 F.2d 272, 277 (6th Cir. 1982)). This rule, however, concerns only the constitutionality of HSI's query of the DEA database and does not squarely address the issue of whether the query violated Section 876. The Government observes that Mr. Hassanshahi "has not identified any statutory or regulatory provision that would proscribe the sharing of information between law enforcement agencies as part of a legitimate law enforcement investigation." Gov't's Feb. 25 Brief at 4–5. Mr. Hassanshahi argues in response that the Government's actions violated Section 876 because the Government "must have known of the unrestricted use of the database while serving the subpoenae (at some point it became obvious that the database was being used for non-drug investigations, but government continued gathering the telephony records)." Def.'s Apr. 13 Brief at 6.

Ultimately, the Court need not determine here who may or may not challenge the statutory validity of the DEA's collection of the metadata or whether Section 876 imposes any limitations on the DEA's ability to share data, because, as discussed, *infra*, the Court finds that,

---

Article III standing in *Clapper* as support. *See* Def.'s June 22 Brief at 15–16. As discussed, *supra* note 3, Article III standing is a separate question not at issue here.

even if Mr. Hassanshahi could challenge the statutory validity of the DEA database, suppression of the evidence would not be an available remedy.

2. Suppression As A Remedy For A Statutory Violation

The Court next turns to the issue of whether, assuming that Mr. Hassanshahi could successfully challenge the statutory validity of the DEA database, the Court could suppress evidence discovered as a result of the database, even if suppression would not be appropriate on constitutional grounds.

The suppression of evidence in a criminal trial is a serious remedy that is ordinarily reserved for certain circumstances involving violations of the Constitution. The Supreme Court has stated that the exclusionary rule "is a prudential doctrine created by this Court to compel respect for the constitutional guaranty." *Davis v. United States*, -- U.S. ----, 131 S. Ct. 2419, 2426 (2011) (internal quotations omitted). On occasion, however, Congress has separately provided a remedy for suppression for statutory violations. *See, e.g., United States v. Donovan*, 429 U.S. 413, 432 (1977) (discussing the statutory suppression remedy provided by 18 U.S.C. § 2515 for violations of 18 U.S.C. § 2518 concerning requirements for wiretaps). Here, Mr. Hassanshahi does not dispute that Congress did not provide a suppression remedy for evidence collected in violation of Section 876. Instead, he argues that the Court should create a suppression remedy on its own. *See* Def.'s Apr. 13 Brief at 8.

In considering this issue, the Court is guided by longstanding principles established by the Supreme Court and followed by the lower courts regarding the exclusionary rule and the suppression of evidence. In *Hudson v. Michigan*, the Supreme Court stated that "[s]uppression of evidence . . . has always been our last resort, not our first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). The Court explained that the rule "generates substantial social costs,

which sometimes include setting the guilty free and the dangerous at large," and that the Court has therefore "been cautious about expanding it and [has] repeatedly emphasized that the rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging its application." *Id.* (internal quotations omitted). The D.C. Circuit has observed that though the Supreme Court "has applied the exclusionary rule to certain Fourth Amendment violations," it "'has never . . . interpreted'" the rule as "'proscrib[ing] the introduction of illegally seized evidence in all proceedings or against all persons.'" *United States v. Spencer*, 530 F.3d 1003, 1006 (D.C. Cir. 2008) (quoting *United States v. Leon*, 468 U.S. 897, 906 (1984)).

This is not to say, however, that the Supreme Court has never suppressed evidence for statutory violations. In *Sanchez-Llamas v. Oregon*, a case decided in the same month as *Hudson*, the Court rejected a petitioner's argument that suppression was required for a violation of the Vienna Convention on Consular Relations, which provides that "when a national of one country is detained by authorities in another, the authorities must notify the consular offices of the detainee's home country if the detainee so requests." *Sanchez-Llamas v. Oregon*, 548 U.S. 331, 338–39 (2006) (citation omitted). In reaching its holding, the Court first observed that it had "applied the exclusionary rule primarily to deter constitutional violations." *Id.* at 348. The Court also noted that in "[t]he few cases in which we have suppressed evidence for statutory violations . . . the excluded evidence arose directly out of statutory violations that implicated important Fourth and Fifth Amendment concerns." *Id.* In its opinion, the Court discussed three such cases. *See id.* at 345 (citing *McNabb v. United States*, 318 U.S. 332 (1943); *Mallory v. United States*, 354 U.S. 449 (1957); *Miller v. United States*, 357 U.S. 301 (1958)).

The Court agrees with the Government's observation that each of these cases, decided in the 1940s and 1950s, "concerned a statute that prophylactically protected Fourth Amendment or

Due Process rights at a time when the judiciary had not fully fleshed out those constitutional protections." Gov't's Feb. 25, 2015 Brief at 7. The Court stated that *McNabb*, for example, "involved the suppression of incriminating statements obtained during a prolonged detention of the defendants, in violation of a statute requiring persons arrested without a warrant to be promptly presented to a judicial officer." [6] *Sanchez-Llamas*, 548 U.S. at 348. As the Court observed, its decisions in *McNabb* and *Mallory* helped later form the foundation for its landmark Fifth Amendment decision in *Miranda*. *See id.* at 348 (citing *Miranda v. Arizona*, 384 U.S. 436, 463 (1966)). Similarly, in *Miller*, the Court "required suppression of evidence that was the product of a search incident to an unlawful arrest." *Id.* at 348–49 (citing *Miller*, 357 U.S. at 305). The D.C. Circuit has recognized that the statute at issue in *Miller* has since merged with judicial interpretation of the Fourth Amendment and that *Miller* is no longer controlling with respect to the availability of a suppression remedy under that statute. *See United States v. Southerland*, 466 F.3d 1083, 1084–86 (D.C. Cir. 2006).

The Court is also guided by decisions of other Circuits holding that suppression is unavailable as a remedy for violations of other statutes. *See, e.g., United States v. Forrester*, 512 F.3d 500, 511–13 (9th Cir. 2007) (holding that suppression is not an available remedy for evidence collected in violation of a pen register statute, in part because "[a]s both the Supreme Court and this court have emphasized, suppression is a disfavored remedy, imposed only where its deterrence benefits outweigh its substantial social costs or (outside the constitutional context) where it is clearly contemplated by the relevant statute); *United States v. Thompson*, 936 F.2d 1249, 1251–52 (11th Cir. 1991) (holding that suppression is not an available remedy for

[6] The Court stated that *Mallory* was similar to *McNabb*, except that it concerned violation of a requirement of a Federal Rule of Criminal Procedure. *See Sanchez-Llamas*, 548 U.S. at 345.

violation of the pen register statute based upon the observation that "several cases indicate that statutory violations by themselves are insufficient to justify the exclusion of any evidence obtained in that manner"), *cert. denied* 502 U.S. 1075 (1992). To the Court's knowledge, no court has ever suppressed evidence because it was collected in violation of Section 876 or, for that matter, in violation of any other administrative subpoena statute that did not explicitly provide for such a remedy.

Mr. Hassanshahi asserts that, in this case, the statutory violation was "intentional and systematic" and argues that this case therefore "presents a case of first impression not governed by *Sanchez-Llamas* or any other government cases." Def.'s Apr. 13 Brief at 8. Following *Clapper*, he argues that it is now clear that the statutory violation implicates the Fourth Amendment and that those implications, together with the statutory violation, require suppression of the evidence. *See* Def.'s June 22 Brief at 12–13. As his sole support for this position, he cites the Second Circuit's discussion of "some of the Fourth Amendment concerns that [the NSA program] implicates" and its statement that "[t]he seriousness of the constitutional concerns . . . has some bearing on" its holding. *Clapper*, 785 F.3d at 821 n.12, 824. He acknowledges, however, that the Second Circuit explicitly declined to reach the "weighty constitutional issues" that it found to be implicated. *Id.* at 824.

The Court disagrees with Mr. Hassanshahi's position that this is a case of first impression not governed by any precedent and regards the extensive precedent concerning the application of the exclusionary rule as instructive. Guided by the Supreme Court's repeated warnings against the expansion of the exclusionary rule even with respect to constitutional violations and the deep aversion of other Circuits to suppress evidence for statutory violations absent a clear indication of congressional intent, the Court declines to create a suppression remedy for evidence collected

in violation of Section 876. The Court is not persuaded by Mr. Hassanshahi's argument that the claimed systematic and intentional statutory violations, together with their Fourth Amendment implications, require suppression. The Court finds that it is unnecessary to expand the exclusionary rule to address these issues and that the Fourth Amendment's well-established exclusionary rule is more than adequate to do so. *Cf. Sanchez-Llamas*, 548 U.S. at 350 ("[W]e think it unnecessary to apply the exclusionary rule where other constitutional and statutory protections—many of them already enforced by the exclusionary rule—safeguard the same interests Sanchez-Llamas claims are advanced by Article 36."). *Clapper*, a decision in a civil case that concerned a different statute and made no mention of the exclusionary rule, does not alter the Court's conclusion.

The Court also notes that even if it were proper to create a suppression remedy for evidence collected through a "systematic and intentional" statutory violation with Fourth Amendment implications, it would be inappropriate to effect such an unprecedented expansion in this case. First, Mr. Hassanshahi seeks to challenge administrative subpoenas directed at third parties. As discussed, *supra*, it is far from clear that he even has the ability to do so, let alone the ability to seek suppression of evidence obtained through a subsequent, separate and constitutional search as a result of those subpoenas. *Cf. Moffett*, 84 F.3d 1294 (rejecting the defendant's attempt to suppress evidence that he claimed was collected from third parties in violation of Section 876, stating that the court's "supervisory power does not authorize us to order suppression of 'otherwise admissible evidence on the ground that it was seized unlawfully from a third party not before the court.'") (quoting *United States v. Payner*, 447 U.S. 727, 735 (1980)). Moreover, the Fourth Amendment implications of the DEA database are also unclear. The Second Circuit observed in *Clapper* that the question of whether individuals have any

privacy rights in records held by third parties that contain metadata relating to their telecommunications "touches an issue on which the Supreme Court's jurisprudence is in some turmoil." *Clapper*, 785 F.3d at 821–25. The "turmoil," however, is somewhat theoretical. As the Foreign Intelligence Surveillance Court explained following *Clapper*, the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which held that individuals have no legitimate expectation of privacy in information that they voluntarily convey to a telecommunications provider when placing a telephone call, remains controlling precedent. *See In re Application of the F.B.I.*, Misc. No. 15-01, 2015 WL 5637562 at **9–13 (FISA Ct. June 29, 2015). The Second Circuit declined to reach "these weighty constitutional issues" in *Clapper*, 785 F.3d at 824, and it would be even less appropriate for the Court to do so here, given that the Court has already assumed the unconstitutionality of the DEA database for purposes of its constitutional analysis and that it is unclear how the suppression analysis for a statutory violation would be any different, as even Mr. Hassanshahi appears to concede at one point. *See* Def.'s Apr. 13 Brief at 9 (arguing that "the Court need not reach the novel issue" in light of the assumption of unconstitutionality).

In conclusion, the Court finds that even if Mr. Hassanshahi had the ability to challenge the statutory validity of the DEA database and could demonstrate that evidence was collected in violation of Section 876—issues the Court does not decide here[7]—suppression of the evidence would not be an available remedy. Therefore, Mr. Hassanshahi is left with his constitutional

[7] To the Court's knowledge, no court has ever ruled on the statutory validity of the DEA's database. The Court also notes that, contrary to Mr. Hassanshahi's assertion that the Second Circuit was unaware of the DEA database at the time of its opinion in *Clapper* and that its decision provides precedent to suppress the evidence here, *see* Def.'s June 22 Brief at 13–17, the Second Circuit in fact explicitly referenced the DEA database in its opinion and declined to "opine as to whether the language of the statute pursuant to which the metadata were collected authorized that program." *Clapper*, 785 F.3d at 812–13 n.6.

challenge to the database as his only avenue for suppressing the evidence recovered from his laptop computer.

B. Mr. Hassanshahi's Constitutional Challenge

The Court next considers whether the newly disclosed details concerning the DEA database and the Second Circuit's decision in *Clapper* require the Court to reverse its prior decision denying Mr. Hassanshahi's motion to suppress the evidence on constitutional grounds.

In its prior decision, the Court explained that under the fruit of the poisonous tree doctrine, an illegal search or seizure requires the exclusion at trial of not only the evidence seized in violation of the Fourth Amendment, but also any evidence obtained as a result of that seizure if the "seizure is a but-for cause of the discovery of the evidence (a necessary condition), and if the causal chain has not become 'too attenuated to justify exclusion,'" *United States v. Brodie*, 742 F.3d 1058, 1062–63 (D.C. Cir. 2014) (quoting *Hudson*, 547 U.S. at 592), "or, to put the same point with another metaphor, if circumstances have not 'purged [the evidence] of the primary taint.'" *Id.* at 1063 (alteration in original) (quoting *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)). The Court held that the exclusionary rule did not require suppression, because "the causal chain leading to the discovery of the laptop evidence was too attenuated to justify exclusion." *Hassanshahi*, 75 F. Supp. 3d at 118 (internal quotation omitted).

In order to determine whether reversal of the Court's decision is required, the Court reviews each stage of its analysis and assesses whether and to what extent the newly disclosed facts and *Clapper* might alter that analysis.

1. Existence Of An Unlawful Search Or Seizure

The Court's preliminary inquiry was whether an unlawful search or seizure occurred. *See Hassanshahi*, 75 F. Supp. 3d at 109. As discussed, the Court assumed that the law enforcement

database and HSI's search of the database were unconstitutional. *See id.* This assumption was, of course, favorable to Mr. Hassanshahi, and the Court maintains that assumption for purposes of its analysis here. The Court need not determine whether the DEA database, as the Court now understands it, was unconstitutional.

2. But-For Causation

The Court also found that the existence of but-for causation was "quite plain." *Hassanshahi*, 75 F. Supp. 3d at 109. The Court need not revisit that finding here, as it was also favorable to Mr. Hassanshahi and remains unchallenged.

3. Attenuation and the Exclusionary Rule

As the Court explained in its prior opinion, the Supreme Court has identified three factors for courts to consider when determining attenuation: (1) the amount of time between the illegality and the discovery of the evidence (i.e., temporal proximity); (2) the presence of intervening circumstances; and (3) the purpose and flagrancy of the illegal conduct. *See Brodie*, 742 F.3d at 1063 (citing *Brown v. Illinois*, 422 U.S. 590, 603–04 (1975)). The Government bears the burden of proving attenuation by a preponderance of the evidence. *See United States v. Holmes*, 505 F.3d 1288, 1293 (D.C. Cir. 2007); *United States v. Wood*, 981 F.2d 536, 541 (D.C. Cir. 1992). The Court reviews its analysis of each of the three factors.

a. Temporal Proximity

The first factor is the temporal proximity between the illegality and the discovery of the evidence. *See Hassanshahi*, 75 F. Supp. 3d at 110 (citing *Brodie*, 742 F.3d at 1063).

The Court observed that the Government's affidavit showed that "more than four months passed between the unconstitutional law enforcement database search on August 24, 2011, and the forensic laptop examination on January 17, 2012." *Id.* (citing Akronowitz Aff. ¶¶ 3, 21, ECF

No. 37-1). The Court found that "this several month gap—during which the Government continued to investigate Hassanshahi through unrelated sources, including the use of preexisting evidence in TECS [a database that the Department of Homeland Security uses in connection with its border inspection processes] and the issuance of lawful subpoenas to Google—weighs in favor of not suppressing the laptop evidence." *Id.*

Neither the new factual details concerning the database nor the Second Circuit's decision in *Clapper* change the Court's factual or legal analysis in any way, nor does Mr. Hassanshahi offer any argument to the contrary. Accordingly, this factor continues to weigh against suppressing the evidence.

b. Intervening Circumstances

The second factor in the attenuation analysis is "whether there were intervening circumstances sufficient to break the causal chain and lessen the taint of the initial illegality." *Hassanshahi*, 75 F. Supp. 3d at 110 (citing *Brodie*, 742 F.3d at 1062–63).

The Court considered two intervening circumstances in its denial of the motion to suppress. First, the Court found that Mr. Hassanshahi's voluntary arrival at LAX in January 2012 was a relevant intervening circumstance, but the Court held that it was "uncertain how much weight to give this event," given the open constitutional question as to whether reasonable suspicion was required for the Government's forensic examination of the laptop. *Id.* at 111–12. The Court held that it did not need to resolve the issue, because a second intervening circumstance, HSI's investigative steps following its discovery of the California telephone number, "unambiguously weighs in favor of not suppressing the laptop evidence." *Id.* at 112.

In making this determination, the Court looked to the "unlawful lead" principle, stating:

> Federal courts have consistently held that the exclusionary rule does not apply to subsequently discovered evidence when an initial

> limited piece of information—typically the name of a potential target for investigation—is obtained through an illegal search or seizure because substantial investigating steps still are required to uncover the necessary incriminating evidence.

Id. The Court acknowledged a long line of cases that have "refus[ed] to apply the exclusionary rule to suppress evidence that was discovered during a later investigation following the initial unlawful discovery of evidence that merely pointed law enforcement in the defendant's direction." *Id.* The Court found that "[t]he circumstances here even more strongly compel finding attenuation than in [those] cases because the law enforcement database revealed only the slimmest of leads: the 818 number." *Id.* at 113.

The Court also observed that, unlike typical "unlawful lead" cases in which the defendant's identity is discovered through the unlawful search, in this case, HSI had to take additional steps to even identify Mr. Hassanshahi. *See id.* The Court found that HSI acted lawfully by then subpoenaing Google for information about the owner of the telephone number and that HSI's subsequent four-month investigation prior to the forensic examination of the laptop "primarily involved the use of information in TECS that existed before the initial database search." *Id.* The Court therefore concluded that "the discovery of the laptop evidence occurred only through substantial and essential intervening events following the 'unlawful lead' that was the 818 number, and this factor therefore weighs strongly in favor of not excluding the evidence." *Id.* This factor was central to the Court's holding. *See id.* at 115 n.6 (stating that "the Court . . . concludes that the attenuation exception applies in large part based on the 'unlawful lead' line of cases").

The newly disclosed details concerning the database do not alter the Court's conclusion in any way; they only bolster it. The Patterson Declaration states that "[n]o subscriber information or other personal identifying information was included in the database" and that it

consisted exclusively of the initiating telephone number, the receiving telephone number, the date, time and location of the call, and the method by which the call was billed. Patterson Decl. ¶ 4. This confirms that, as the Court found in its prior opinion, the DEA database provided HSI with only "the slimmest of leads" and that HSI had to conduct a further investigation to even identify Mr. Hassanshahi.

Mr. Hassanshahi challenges the Court's conclusion, claiming that the Government has not "come clean even at this stage." Def.'s Apr. 13 Brief at 6. He relies upon a news report published by Reuters on August 5, 2013 concerning "[a] secretive U.S. Drug Enforcement Administration unit" called the Special Operations Division ("SOD") that the report states "is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans." *Id.* (quoting Def.'s Apr. 13 Brief Ex. at 1, ECF No. 53-1). The news report purports to rely on a secret Government document that instructs agents to "omit the SOD's involvement from investigative reports, affidavits, discussions with prosecutors and courtroom testimony" and to "use normal investigative techniques to recreate the information provided by SOD." *Id.* at 6–7 (quoting Def.'s Apr. 13 Brief Ex. at 2). Mr. Hassanshahi suggests that the Government's disclosure of its subsequent search of TECS in a supplemental affidavit submitted in opposition to his motion to suppress may have been "an attempt to 'recreate' an investigative trail that originated with SOD[.]" On this issue, the Government states that "[w]hile it would not be improper for a law enforcement agency to take steps to protect the confidentiality of a law enforcement sensitive investigative technique, this case raises no such issue." Gov't's Feb. 25 Brief at 3, n.2.

Though the Court does not necessarily share the Government's view regarding the propriety of the "recreation" technique, particularly if doing so involves providing false or misleading information to a criminal defendant or the Court, the Court finds no basis for concluding that the Government employed that technique here. Most significantly, Mr. Hassanshahi's theory is belied by the fact that the Government disclosed the existence of the database at issue here, albeit with limited detail, from the very beginning of its prosecution. *See* Aff. In Support Of Criminal Compl. ¶ 15, ECF No. 1-1 ("Using the business telephone number associated with 'Sheikhi', I searched HSI-accessible law enforcement databases . . . ."). Had the Government recreated its investigative steps to conceal potentially unlawful actions, it is hard to believe that the Government would have freely made this disclosure. Moreover, the Court already addressed Mr. Hassanshahi's issue with respect to the timing and nature of the Government's disclosure regarding the TECS database search in its opinion denying his motion to suppress, as Mr. Hassanshahi first raised it at oral argument on his motion. *See Hassanshahi*, 75 F. Supp. 3d at 105 n.1 (finding that "the second affidavit merely provides more information about the HSI investigation than the first affidavit, which is not surprising given the different purposes").

The Court is thus satisfied that the newly disclosed information concerning the database does not alter its conclusion that the Government's investigative steps following the discovery of the California telephone number, a minor lead in the case, constitute an intervening circumstance that weighs heavily and unambiguously against suppressing the laptop evidence.

c. Purpose And Flagrancy Of The Illegal Conduct

The final factor in the attenuation analysis is the "purpose" and "flagrancy" of the illegal law enforcement conduct. *See Hassanshahi*, 75 F. Supp. 3d at 101 (citing *Brodie*, 742 F.3d at

1063). "As a rule, courts generally 'favor suppression' only 'if law enforcement officials conducted the illegal search with the purpose of extracting evidence against the defendant, or if they flagrantly broke the law in conducting the search.'" *Id.* (quoting *United States v. Washington*, 387 F.3d 1060, 1075 (9th Cir. 2004)). Though the Court acknowledged that it was "left slightly in the dark regarding the flagrancy element" given the lack of detail provided by the Government at the time, the Court nevertheless unequivocally concluded that "HSI did not act purposefully or in bad faith to violate Hassanshahi's constitutional rights." *Id.* at 114–15. In making this determination, the Court took several factors into account.

First, the Court "surmise[d] . . . that the law enforcement database operates fairly similarly to the NSA program, at least insofar as the database appears to include a repository of aggregated telephone records for calls made into the U.S. from abroad." *Id.* at 114. The Court stated, however, that the "ambiguity" regarding the nature of the database complicated its analysis. *Id.* The Court explained that if, for example, it treated the database as "functionally equivalent to the NSA telephony program," then the Court would "likely conclude that HSI acted in good faith," because courts had generally approved of the program and, at the time of HSI's search of the database, no court had deemed the program unconstitutional. *Id.*

The Court stated, however, that it did not "know with certainty whether the HSI database actually involves the same public interests, characteristics, and limitations as the NSA program such that both databases should be regarded similarly under the Fourth Amendment." *Id.* In particular, the Court noted that the NSA database "was specifically limited to being used for counterterrorism purposes, and it remains unclear if the database that HSI searched imposed a similar counterterrorism requirement." *Id.* The Court speculated broadly that "[i]f the HSI database did have such a limitation, that might suggest some level of flagrancy by HSI because it

was clear that neither Sheikhi nor Hassanshahi was involved in counterterrorism activities." *Id.* The Court nevertheless concluded that "even assuming that the HSI database was misused to develop the lead into Hassanshahi, HSI's conduct appears no more flagrant than law enforcement conduct in other 'unlawful lead' cases, which still held that the attenuation exception applied nonetheless." *Id.* at 114–15 (citing *United States v. Carter*, 573 F.3d 418, 421 (7th Cir. 2009) (admitting evidence after illegal search of defendant's residence); *United States v. Smith*, 155 F.3d 1051, 1059 (9th Cir. 1998) (admitting evidence resulting from an "illegally intercepted wire communication"); *United States v. Friedland*, 441 F.2d 855, 856 (2d Cir. 1971) (admitting evidence after the "FBI unlawfully installed electronic 'bugs'" in an office)).

The Court stated that it was "more certain, though, that HSI did not search the law enforcement database for the purpose of 'extracting evidence against the defendant.'" *Id.* at 115 (quoting *Washington*, 387 F.3d at 1075). The Court based this determination on the fact that, when it searched the database, "HSI had no inclination that Hassanshahi was involved" and that "the agency used the law enforcement database to cast a wide net for potential U.S.-based suspects." *Id.* Based largely on this determination, the Court found that the "purpose" and "flagrancy" factor weighed against suppressing the evidence.

Mr. Hassanshahi argues that the newly disclosed information concerning the database should materially alter the Court's analysis of this factor. He argues that the newly disclosed information demonstrates that the Government's actions were "nothing *but* purposeful," because: the Government "essentially subpoenaed 100% of Americans' telephony data and metadata for *decades*, without any specific investigation pending, all in deliberate violation of the statute"; the Government made the database "available to any and all comers, in deliberate violation" of the statute; the Government took steps to conceal the true source of the information; and the

Government "did all this deliberately, purposefully and systematically, all while knowing *for certain* of the statutory violations and with strong knowledge of the Fourth Amendment implications if not outright violations." Def.'s July 29 Brief at 3–4. He principally relies on the Seventh Circuit's opinion in *United States v. Reed*, 349 F.3d 457, 464–65 (7th Cir. 2003) regarding the importance of the purpose and flagrancy factor and argues that the flagrancy and purposefulness of the Government's conduct in this case "far exceeds, in depth and scope, any one-time violation such as was found flagrant in cases like *Reed*." Def.'s July 29 Brief at 3–4.

The Court is not persuaded. As a preliminary matter, nearly all of Mr. Hassanshahi's points concern whether the Government purposefully violated Section 876, not the relevant inquiry of whether it purposefully violated the Constitution. Moreover, Mr. Hassanshahi's factual assertions have little, if any, basis in the record. For example, the record does not indicate that the Government "essentially subpoenaed 100% of Americans' telephony data and metadata for decades." On the contrary, the Patterson Declaration states that the metadata concerned only calls originating from the United States and calling foreign countries. *See* Patterson Decl. ¶ 4. Also, as discussed, *supra*, there is no indication here that the Government has taken any steps to conceal the true source of the information, and Mr. Hassanshahi offers no support for his assertion that the Government "[knew] for certain" that it was violating a statute, which no court has ever decided. Mr. Hassanshahi's reliance on *Reed* is also misplaced. First, contrary to Mr. Hassanshahi's assertions, the Seventh Circuit did not hold that the misconduct in that case required suppression; it remanded the case to the district court to consider whether the unlawful actions were taken to advance the investigation or "embark on a fishing expedition" as "relevant" to the suppression analysis. *Reed*, 349 F.3d at 465–66. Second, in *Reed*, unlike this case, the Seventh Circuit upheld the district court's determination that there were "no intervening

circumstances sufficient to purge the taint of the allegedly illegal arrest." *Id.* at 464. As explained, *supra*, the Court's finding of intervening circumstances in this case weighs heavily against suppression and is central to its holding.

Perhaps the most glaring flaw in Mr. Hassanshahi's briefing on this issue is his failure to engage with the Court's prior analysis of the purpose and flagrancy factor and demonstrate what exactly about the new information should alter the Court's analysis. For the sake of clarity, however, the Court will revisit its analysis in light of the new information and *Clapper*.

Most significantly, the newly disclosed information does not in any way change the Court's critical conclusion that HSI did not search the law enforcement database in order to target Mr. Hassanshahi. Regardless of any other factual developments since the Court's prior opinion, it remains clear that when HSI searched the DEA database, it had no indication that Mr. Hassanshahi had any involvement in the matters it was investigating and that HSI was unable to even identify Mr. Hassanshahi until after it lawfully obtained information from Google. Given that the Court concluded on this basis that the purpose and flagrancy factor counseled against suppression, this is sufficient for the Court to determine that reconsideration of this factor is unjustified.

Nevertheless, the Court observes that the newly disclosed information resolves some of the ambiguity described in the Court's prior opinion concerning whether the Court could treat the database at issue here as "functionally equivalent" to the NSA's database and whether HSI "misused" the database to develop the lead into Mr. Hassanshahi. It is now clearer that the DEA database was similar in many important respects to the NSA's database. For instance, the Patterson Declaration largely confirms the Court's hypothesis that the DEA database contained records of international telephone calls, except the Court now understands that the records

concerned calls originating in the United States, rather than abroad. *See* Patterson Decl. ¶ 4. The Court also now understands that the records were limited to specific types of metadata that did not include any personal identifying information. These records appear to have actually been narrower in scope than the records stored in the NSA's telephony database. *See Clapper*, 785 F.3d at 793–97 (describing orders under the NSA program calling for "all call-detail records or 'telephony metadata'" of all domestic and international calls).

The DEA database also appears to have differed in some other ways. Most notably, the Court now understands that the DEA originally collected the information contained in the database and that HSI accessed it for a different purpose. [8] *See* Patterson Decl. ¶ 5. Though the Court speculated in its prior opinion that if the database was limited to a purpose not relevant here, it "might suggest some level of flagrancy," the Court is satisfied, upon consideration of the supplemental briefing on this issue, that HSI's subsequent search of the database does not suggest that the Government purposefully and flagrantly violated the Fourth Amendment, given well-established precedent that "[e]vidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken." *Jabara*, 691 F.2d at 277. *See also Johnson v. Quander*, 440 F.3d 489, 498–500 (D.C. Cir. 2006) (holding that the Government's access to a database containing a defendant's "genetic fingerprint" lawfully collected while he was on probation after the defendant's probation terminated and for a different purpose did not constitute a separate search for Fourth Amendment purposes). Moreover, as the Court explained in its prior opinion, even

[8] Mr. Hassanshahi also observes that the NSA's program involved oversight by the Foreign Intelligence Surveillance Court, whereas the DEA's database was compiled using administrative subpoenas, yet he does not offer any reason to find that the use of administrative subpoenas—a well-established and legitimate power authorized by Congress—suggests a flagrant constitutional violation. *See* Def.'s June 22 Brief at 6–7.

assuming that HSI "misused" the DEA database, its conduct appears no less flagrant than other "unlawful lead" cases in which courts have applied the attenuation exception. *See Hassanshahi*, 75 F. Supp. 3d at 114–15.

In its prior opinion, the Court stated that if it treated the database at issue as "functionally equivalent" to the NSA's program, then it would likely conclude that HSI acted in good faith, because courts have generally approved of the NSA's program and because no court at the time of the search had disapproved of it. Cases decided since the Court's opinion do not require any alteration to that analysis. The Court noted that the one exception at the time of its decision was Judge Leon's opinion in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013). The D.C. Circuit has since vacated that decision on standing grounds. *See Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015). Nor does the Second Circuit's decision in *Clapper* affect the Court's prior analysis, as the Second Circuit declined to reach the constitutional issues in that case. Though there are differences between the two, the Court is now more comfortable viewing the DEA database and the NSA's program as "functionally equivalent" for purposes of the Court's analysis here, which only bolsters the Court's earlier conclusion regarding the purpose and flagrancy factor of the attenuation analysis.

* * * *

In sum, while the newly disclosed information concerning the DEA database provides helpful clarity, the Court finds that none of the new information, nor *Clapper* or any other developments in the legal landscape, alter the Court's prior conclusion that all three attenuation factors weigh against suppression and that the new information only confirms the Court's prior

holding that the exclusionary rule does not require suppressing the laptop evidence in this case as fruit of the poisonous tree.[9]

V. CONCLUSION

For the foregoing reasons, Defendant Shantia Hassanshahi's motion for reconsideration is **DENIED**.

SO ORDERED.

Dated: November 19, 2015

RUDOLPH CONTRERAS
United States District Judge

[9] The Court also rejects Mr. Hassanshahi's request, in the alternative, for an evidentiary hearing to explore "the extent and operation" of the DEA database. Def.'s June 22 Brief at 17. The Court finds that, for the reasons provided in this opinion and in the Court's prior opinion, Mr. Hassanshahi has not identified any unresolved factual issues that could alter the Court's conclusion.