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,	:	Re Document No.: 28
also known as Shahi,	:	
also known as Shantia Haas,	:	
also known as Sean Haas,	:	
	:	
and	:	
	:	
HASSTON, INC.,	:	
	:	
Defendants.	:	

MEMORANDUM OPINION

DENYING DEFENDANT'S MOTION TO SUPPRESS

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. Now before the Court is Hassanshahi's motion to suppress evidence uncovered during a forensic examination of his laptop following an international border stop at Los Angeles International Airport on the basis that the laptop examination violated the Fourth Amendment. Upon consideration of Hassanshahi's motion and the opposition thereto, the Court reaches two conclusions: first, the exclusionary rule does not require suppressing the laptop evidence as fruit of the poisonous tree because discovery of that evidence was sufficiently attenuated from the initial unlawful telephone database search; and second, reasonable suspicion

existed for conducting the forensic examination after Hassanshahi landed at the airport. Accordingly, the Court will deny Hassanshahi's motion to suppress.

II. FACTUAL BACKGROUND[1]

On August 16, 2011, Homeland Security Investigations ("HSI") received an unsolicited e-mail from a source indicating that the source had received an e-mail from an Iranian known as M. Sheikhi who, on behalf of his Iranian company, sought the source's assistance in procuring protection relays for an Iranian power project. *See* Akronowitz Aff., ECF No. 37-1 ("2d Akronowitz Aff.") at ¶ 2. The e-mail from Sheikhi to the source contained an Iranian business telephone number and the address for Sheikhi's company in Tehran, Iran. *See id*. An HSI agent used the telephone number associated with Sheikhi to search an "HSI-accessible law enforcement database" in the hope of identifying potential U.S.-based targets engaged in the sale or export of protection relays for use in Iran. *See id*. ¶ 3. The HSI agent's search returned a single telephone record indicating one call between Sheikhi's telephone number and a telephone number with an "818" area code (the "818 number"), which is the area code for Los Angeles, California. *See id*. ¶ 4.

[1] The United States of America (the "Government") provides the following facts through affidavits submitted by HSI Special Agent Akronowitz. At oral argument, Hassanshahi objected to the Government's provision of the Akronowitz affidavits by arguing that the affidavits were internally inconsistent and, by implication, unreliable or simply untruthful. The Court is satisfied, however, by the Government's explanation that the first Akronowitz affidavit was prepared to support the criminal complaint and the second, more detailed Akronowitz affidavit was prepared to support the Government's opposition to the motion to suppress. Hassanshahi has provided no legal basis for why the Government was not entitled to submit a supplemental affidavit in response to the motion to suppress, and the Court finds that there is nothing internally inconsistent between the affidavits — the second affidavit merely provides more information about the HSI investigation than the first affidavit, which is not surprising given the different purposes. Finally, the fact that the Government later provided a third, corrected Akronowitz affidavit does not render the earlier affidavits defective or unreliable in their entirety.

After discovering that the 818 number was assigned to Google/Google Voice, *see id*. ¶ 13, HSI prepared and served on Google an Administrative Export Enforcement Control Subpoena ("AEEC Subpoena"). *See id*. ¶ 14. In response, Google provided information that identified Hassanshahi as the person to whom the 818 number was registered, and Google also provided an e-mail address registered to Hassanshahi. *See id*. ¶ 15. In addition, Google provided call log information for the period between September 6, 2011, and October 6, 2011, which showed that the 818 number had received one telephone call from an unknown Iranian phone number on October 5, 2011. *See id.*; Revised Akronowitz Aff., ECF No. 42-1 ("3d Akronowitz Aff.") at ¶ 15. The Google call log information also revealed one missed call between Hassanshahi's 818 number and an unknown Iranian cell phone number on September 19, 2011. *See* 2d Akronowitz Aff. ¶ 15.

On October 18, 2011, the HSI agent searched the Department of Homeland Security's ("DHS") TECS database for additional information about Hassanshahi.[2] *See id*. ¶ 16. TECS led the agent to discover that Hassanshahi was involved in a prior federal law enforcement investigation into potential violations of the Iran trade embargo.[3] *See id*. ¶ 16a. Specifically, the

[2] TECS is a database that serves as a data repository to support law enforcement "lookouts," border screening, and reporting for DHS's primary and secondary border inspection processes. *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.

[3] The HSI agent's affidavit does not state that this information about the 2003 investigation actually was written in TECS. Instead, the affidavit merely provides that after "conduct[ing] research on Hassanshahi in TECS," the HSI agent "discovered" the information about the 2003 investigation. *See* 2d Akronowitz Aff. ¶ 16. At oral argument on the motion to suppress, counsel for the Government suggested that the HSI agent discovered the information about the investigation through a telephone call with another agent, a call that is not referenced anywhere in the affidavit. The affidavit also does not specify if or when the HSI agent reviewed HSI's investigative file from the 2003 investigation. In fact, counsel for the Government stated at oral argument that the 2003 HSI investigative file had not yet been produced to Hassanshahi as part of discovery in this criminal case. As such, it remains somewhat ambiguous and open for further clarification how the HSI agent learned the information about the 2003 investigation that he put in his affidavit, as well as how much the HSI agent actually knew about this investigation

investigation occurred in 2003 through an HSI office in California, and the investigation uncovered that Hassanshahi and two partners had established an American company for the purpose of entering into an agreement with a Chinese company to build a computer production facility in Iran. *See id.* Hassanshahi's American company later filed a breach-of-contract claim against the Chinese company in California state court, and that lawsuit was dismissed in part because the contract was unenforceable as against public policy since it involved doing business in Iran, a clear violation of U.S. law. *See id*. The Department of Justice did not file criminal charges against Hassanshahi for his role in this venture. *See id.*

The TECS search also revealed a number of earlier instances in which Hassanshahi reentered the U.S. after traveling to the Middle East, including: an incident in 2005 when Hassanshahi was questioned by U.S. Customs and Border Protection ("CBP") agents after returning from Dubai with $15,000 in cash; an incident in 2006 when Hassanshahi returned from Tehran with a travel companion; and four other returns from Tehran — two in 2008, one in 2010, and one in May 2011. *See id*. ¶¶ 16c-e. In addition, HSI learned through TECS that Hassanshahi presently was outside the U.S., so HSI supplemented the existing TECS information by entering instructions that HSI should be alerted and Hassanshahi should be referred for secondary screening the next time he returned to the U.S. *See id*. ¶ 17.

Around December 20, 2011, HSI served Google with a second AEEC Subpoena, this time seeking subscriber information and recent Internet protocol ("IP") logs for Hassanshahi's Google e-mail account. *See id*. ¶ 18. In response, Google provided information indicating that Hassanshahi's e-mail account was accessed from an Iran IP address twenty-four times between

---

before ordering the forensic examination in January 2012. Nonetheless, for the purposes of the motion to suppress, the Court accepts that the HSI agent knew the details about the 2003 investigation that he provides in the affidavit.

December 8, 2011, and December 15, 2011. *See id.* The information provided by Google also showed, however, that Hassanshahi's e-mail account was accessed from a U.S. IP address on the same day it apparently was accessed from an Iran IP address, including sometimes within just a few minutes of each other. *See* Def.'s Reply Supp. Mot. Dismiss Ex. 1 at 27 (Google Subscriber Information). And on another occasion, Hassanshahi's e-mail account apparently was accessed on the same day from an Iran IP address, a Germany IP address, and a U.S. IP address, occasionally alternating between the countries within minutes. *See id.* at 30.

On January 11, 2012, HSI was alerted that Hassanshahi would be returning to the U.S. the next day through Los Angeles International Airport ("LAX"). *See* 2d Akronowitz Aff. ¶ 19. When Hassanshahi arrived at LAX on January 12, he was referred for secondary screening, at which time CBP agents seized several electronic devices in Hassanshahi's possession — including a laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone — and sent those devices to the HSI agent in Sterling, Virginia, for further analysis.[4] *See id.* ¶ 20; Arkonowitz Aff., ECF No. 1-1 ("1st Arkonowitz Aff.") at ¶ 19. When the devices arrived in Virginia a few days later, HSI conducted a forensic examination of the laptop and discovered numerous documents relating to Hassanshahi's apparent business activities in Iran, *see* 2d Arkonowitz Aff. ¶ 21, including documents showing that in 2009, Hassanshahi, through his company, purchased approximately $6,000,000 in goods that were exported to Armenia and then transshipped to Iran, *see* 1st Arkonowitz Aff. ¶ 22, as well as a September 5, 2011, letter from Hassanshahi to the Iranian Minister of Energy in which Hassanshahi asked the Iranian government for payment for "protective relays for transmission lines." *See id.*

[4] Hassanshahi also possessed "approximately" $7,000 in cash when he arrived at LAX on January 12, 2012. *See* Def.'s Reply Supp. Mot. Suppress Ex. 1 at 48.

Now before the Court is Hassanshahi's motion to suppress the evidence discovered during the forensic examination of his laptop. Hassanshahi asserts two arguments in support of his motion. First, he argues that the law enforcement database through which HSI initially obtained his 818 number constituted an unconstitutional search, and under the fruit of the poisonous tree doctrine, the forensic laptop examination was the direct result of that unlawful search such that the laptop evidence was tainted and must be suppressed. Second and alternatively, Hassanshahi argues that this Court should follow two recent court decisions from other federal jurisdictions that concluded that the Fourth Amendment required reasonable suspicion to conduct a forensic examination of an electronic device after an international border stop.[5] Hassanshahi then argues that the laptop evidence must be suppressed here because the Government lacked reasonable suspicion for the search. The Court addresses these arguments below.

III. ANALYSIS

Hassanshahi's motion to suppress requires the Court to analyze two important areas of Fourth Amendment jurisprudence: the fruit of the poisonous tree doctrine and international border searches. As to the first issue, it is well settled that evidence secured as the result of an illegal search or seizure is tainted fruit of a poisonous tree that must be suppressed, unless intervening events or other attenuating circumstances sufficiently dissipated the taint of the initial illegality. The Court ultimately finds that such attenuating circumstances existed here, and the exclusionary rule therefore does not require suppression of the evidence found on

[5] *See generally United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), *cert. denied*, 134 S. Ct. 899 (2014), *reh'g denied*, 134 S. Ct. 1512 (2014); *United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014), *reconsideration denied*, No. CRIM. PWG-13-100, 2014 WL 3741141 (D. Md. July 28, 2014).

Hassanshahi's laptop. Second, the Court finds that reasonable suspicion existed for the forensic examination of Hassanshahi's laptop after it was seized during the international border stop at LAX. Finally, because the Court reaches this conclusion as to reasonable suspicion, it need not — and does not — take a position regarding whether, as a matter of law, the Fourth Amendment required the Government to possess reasonable suspicion before conducting the forensic examination.

A. Legal Standard For Motion To Suppress

Generally, "[t]he proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure." *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978) (citations omitted). However, when, like here, "'a defendant produces evidence that he was arrested or subjected to a search without a warrant, the burden shifts to the government to justify the warrantless arrest or search.'" *United States v. Jones*, 374 F. Supp. 2d 143, 147 (D.D.C. 2005) (quoting *United States v. de la Fuente*, 548 F.2d 528, 533 (5th Cir. 1977)); *see also United States v. Jeffers*, 342 U.S. 48, 51 (1951) ("[T]he burden is on those seeking the exemption to show the need for it[.]" (citation omitted)); *United States v. Mangum*, 100 F.3d 164, 169 (D.C. Cir. 1996) ("The government carries the burden of showing that the measures employed during the stop were justified.").

B. Fruit Of The Poisonous Tree And Attenuation

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. By its text, the Amendment "'contains no provision expressly precluding the use of evidence obtained in violation of its commands.'" *Herring v. United States*, 555 U.S. 135, 139 (2009) (quoting *Arizona v. Evans*, 514 U.S. 1, 10 (1995)). Supreme Court decisions, however, have

"establish[ed] an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial," *see id*., in order "to 'compel respect for the constitutional guaranty.'" *Davis v. United States*, 131 S. Ct. 2419, 2426 (2011) (quoting *Elkins v. United States*, 364 U.S. 206, 217 (1960)). Furthermore, though the Supreme Court "has applied the exclusionary rule to certain Fourth Amendment violations[,]" it "'has never … interpreted'" that 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)). Rather, the exclusionary rule is designed to safeguard Fourth Amendment rights through its deterrent effect, and the rule therefore only applies when it results in "appreciable deterrence." *See Herring*, 555 U.S. at 139-41.

The fruit of the poisonous tree doctrine was developed within the context of the Supreme Court's exclusionary rule jurisprudence. Under the 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 v. Michigan*, 547 U.S. 586, 592 (2006)), "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)). In the motion to suppress, Hassanshahi argues that the evidence on his laptop should be excluded as tainted fruit because its discovery resulted directly from the initial law enforcement database search that uncovered the 818 number.

1. Existence Of An Initial Unlawful Search Or Seizure

The Court's preliminary inquiry is whether an unlawful search or seizure occurred. Hassanshahi argues that the law enforcement database in which the HSI agent ran a search using Sheikhi's business telephone number must be either the National Security Agency's ("NSA") bulk telephony metadata program or an equivalent telephony database. *See* Def.'s Mem. Supp. Mot. Suppress 18-30. Hassanshahi then relies on Judge Leon's opinion in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *appeal pending*, No. 14-5004 (D.C. Cir.), to establish the facial unconstitutionality of the NSA telephony program or, by implication, the unconstitutionality of the unknown equivalent database allegedly used by HSI here.

In response, the Government sidesteps Hassanshahi's argument by taking the position that although the NSA telephony database was not used, the Court nevertheless should assume *arguendo* that the law enforcement database HSI did use was unconstitutional. *See* Gov't's Mem. Opp'n Mot. Suppress 12. Consistent with this position, the Government refuses to provide details about its law enforcement database on the basis that such information is irrelevant once the Court accepts the facial illegality of the database. *See id*. at 11-12. Regrettably, the Court therefore starts its analysis from the posture that HSI's initial search of the mysterious law enforcement database, which uncovered one call between Sheikhi's business telephone number and the 818 number linked to Hassanshahi, was unconstitutional.

2. But-For Causation

Next, the Court finds that the existence of but-for causation between the law enforcement database search and the forensic laptop examination is quite plain. *See Brodie*, 742 F.3d at 1062-63 (explaining that "but-for" causation is a "necessary condition" in the fruit of the poisonous tree analysis); *see also Owens v. Republic of Sudan*, 412 F. Supp. 2d 99, 111 (D.D.C. 2006) (but-

for causation asks: "were the act removed from the sequence of events leading up to the injury, would the injury have occurred as it did?"). Here, the law enforcement database search revealed the 818 number, which led HSI to subpoena Google, through which HSI learned that the 818 number was registered to Hassanshahi. HSI then investigated Hassanshahi through TECS and by issuing a second subpoena to Google, which together led HSI to place an alert in TECS requiring CBP officers to refer Hassanshahi for secondary screening the next time he returned to the U.S. Finally, when Hassanshahi arrived at LAX, CBP officers followed the TECS instruction by referring Hassanshahi to secondary screening, and Hassanshahi's laptop then was seized and sent to Virginia for the forensic examination. As such, the Court easily concludes that "but for" the initial law enforcement database search, the forensic laptop examination would not have occurred.

3. Attenuation And The Exclusionary Rule

"[N]ot … all evidence is 'fruit of the poisonous tree' simply because it would not have come to light but for the illegal actions of the police." *Wong Sun*, 371 U.S. at 487-88. Instead, exclusion is not required when "the government proves … that the evidence would have been discovered inevitably, was discovered through independent means, or that its discovery was so attenuated from the illegal search or seizure that the taint of the unlawful government conduct was dissipated." *United States v. Holmes*, 505 F.3d 1288, 1293 (D.C. Cir. 2007) (citations omitted). Here, the Government argues that attenuation existed, and 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 Holmes*, 505 F.3d at 1293; *United States v. Wood*, 981 F.2d 536, 541 (D.C. Cir. 1992).

a. Temporal Proximity

The Court first considers the temporal proximity between the illegality and the discovery of the evidence. *See Brodie*, 742 F.3d at 1063. The Government's affidavit shows 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. *See* 2d Akronowitz Aff. ¶¶ 3, 21. Though "there is no 'bright-line' test for temporal proximity" within the attenuation analysis, *see United States v. Reed*, 349 F.3d 457, 463 (7th Cir. 2003), the Court finds that this several month gap — during which the Government continued to investigate Hassanshahi through unrelated sources, including the use of preexisting evidence in TECS and the issuance of lawful subpoenas to Google — weighs in favor of not suppressing the laptop evidence. *Compare United States v. Gross*, 662 F.3d 393, 402 (6th Cir. 2011) (finding that two month gap between the unlawful seizure and defendant's voluntary confession suggests attenuation as to the confession), *United States v. Roberts*, No. 11-CR-0018, 2012 WL 1033515, at *7 (E.D. Pa. Mar. 28, 2012) (finding that the "temporal proximity" factor weighed against suppression when over two months elapsed between the initial unlawful search and defendant's consent to a second search that revealed incriminating evidence), *and United States v. Lawrence*, No. CRIM.05-333, 2006 WL 752920, at *6 (D. Minn. Mar. 23, 2006) (finding attenuation in part because four months passed between the illegal search and arrest and the later incriminating statements made by defendant), *with United States v. Miller*, 146 F.3d 274, 280 (5th Cir. 1998) (finding that the ninety second time period between the illegal stop and the search did not support the government's attenuation claim), *United States v. Green*, 111 F.3d 515, 521 (7th Cir.

1997) (explaining that the fact that only five minutes elapsed between the illegal stop and the search of the car weighed against attenuation), *and United States v. Ceballos*, 812 F.2d 42, 50 (2d Cir. 1987) (finding that "the [consent] to search and the statements given were too closely connected in context and time … to break the chain of illegality" when only a few minutes had elapsed).

b. Intervening Circumstances

The Court next considers whether there were intervening circumstances sufficient to break the causal chain and lessen the taint of the initial illegality. *See Brodie*, 742 F.3d at 1062-63. Often, the intervening circumstance that most strongly dissipates the evidentiary taint is a "voluntary act by the defendant." *Green*, 111 F.3d at 522; *see also United States v. Jackson*, No. A04-141 CR, 2005 WL 1115466, at *17 (D. Alaska May 10, 2005) ("A defendant may himself commit an intervening independent act that will be sufficient in relation to other events for attenuation purposes." (citing United States v. Sprinkle, 106 F.3d 613, 619 (4th Cir. 1997)). In opposition to Hassanshahi's motion to suppress, the Government offers two intervening events: HSI's investigative steps following discovery of the 818 number, which itself was just a minor lead in the case; and Hassanshahi's voluntary appearance at LAX after arriving on an international flight. *See* Gov't's Mem. Opp'n Mot. Suppress 13.

i. Hassanshahi's Arrival At LAX

Starting with the latter event, the Court finds that Hassanshahi's voluntary arrival at LAX was a relevant intervening circumstance, but at the same time, the Court is uncertain how much weight to give this event. Because Hassanshahi's arrival at LAX on an inbound international flight provided the Government with justification to conduct a border search, this situation is somewhat analogous to the more common instance in which a defendant, through new conduct

following an unlawful search or seizure, gives the police a fresh basis for conducting a legal search or seizure. For example, in *United States v. Sprinkle*, 106 F.3d 613 (4th Cir. 1997), the Fourth Circuit held that when the defendant fled from and fired a gun at an officer while resisting an unjustified investigative stop, the defendant committed a new crime that "purged the taint of the prior illegal stop" and provided the officer with probable cause to arrest the defendant and then seize a gun that was in plain view at the scene of the new crime. *Id.* at 619.

Similarly, in *United States v. Jackson*, No. A04-141 CR, 2005 WL 1115466 (D. Alaska May 10, 2005), the district court held that when the defendant disobeyed an order by a uniformed officer during an unlawful stop and fled down the street, the officer acquired new and sufficient justification to pursue the fleeing defendant, seize the defendant, and then conduct a pat-down search of the defendant, which revealed contraband in the defendant's possession. *Id*. at *14-16; *see also United States v. Allen*, 619 F.3d 518, 526 (6th Cir. 2010) ("Here, there was an initial attempt at a traffic stop, which [the defendant] claims to have been illegal, followed by an attempt to escape from the police by leading the officers on a high-speed chase…. [T]he act of fleeing from police officers constituted a new, distinct crime that rendered evidence subsequently seized admissible."); *United States v. Hooker*, No. 94-5863, 54 F.3d 774, *2 (4th Cir. 1995) (finding that defendant's "voluntary action" of coming out of her home, approaching the officers, and stating that her "conscience" was bothering her and the officers thus could enter and search her home were adequate intervening circumstances to purge taint of the earlier unlawful seizure and search of defendant's car).

As these cases illustrate, a voluntary act by a person following initial unlawful law enforcement conduct can provide an officer with new grounds for conducting a lawful search or seizure such that the exclusionary rule does not apply to any newly recovered evidence. This

concept, however, may get the Government only so far: though Hassanshahi's arrival at LAX provided justification to conduct a border search, Hassanshahi argues that the forensic laptop examination went beyond a routine suspicionless border search and therefore required reasonable suspicion. Accepting *arguendo* that reasonable suspicion in fact was required, Hassanshahi's arrival at LAX would be one factor in the reasonable suspicion calculus, but landing at LAX, by itself, would not have created reasonable suspicion for the forensic examination. As such, the circumstances here would be distinguishable from the typical case in which the intervening voluntary conduct provided all the cause or suspicion that was required for the second search or seizure. On the other hand, if the Court rejects Hassanshahi's argument that reasonable suspicion was required, his arrival at LAX alone would have justified the forensic examination, thus making the arrival a more significant, and perhaps even dispositive, attenuating circumstance. The Court ultimately need not resolve this issue, however, because the Government's other intervening circumstance argument unambiguously weighs heavily in favor of not suppressing the laptop evidence.

ii. The 818 Number "Lead" And The Need For Further Investigation

Federal courts consistently have 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 intervening investigative steps still are required to uncover the necessary incriminating evidence. The seminal case on this "unlawful lead" principle came from Judge Friendly in *United States v. Friedland*, 441 F.2d 855 (2d Cir. 1971). There, federal officers illegally bugged the offices of the defendant's acquaintance, and those officers then informed other agents that the defendant should be investigated based on conversations the officers illicitly

overheard. *See id*. at 854-57. In refusing to suppress inculpatory evidence about the defendant that was discovered through further lawful investigation, the court held that it "would stretch the exclusionary rule beyond tolerable bounds" to "grant life-long immunity from investigation and prosecution simply because a violation of the Fourth Amendment first indicated to the police that a man was not the law-abiding citizen he purported to be." *Id*. at 861.

Other courts have taken a similar approach since *Friedland* by refusing 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. For instance, in *United States v. Carter*, 573 F.3d 418 (7th Cir. 2009), the court explained that "[f]ew cases, if any, applying the attenuation exception hold that evidence separately uncovered through completely lawful means is inadmissible because an illegal search first made a particular person a suspect in a criminal investigation." *Id*. at 423. The court then concluded that an out-of-court identification was admissible under the attenuation exception even though law enforcement's original interest in the defendant arose through the discovery of an "Inmate ID Card" bearing the defendant's name during a prior unlawful search. *Id*. at 420, 423.

Similarly, in *United States v. Watson*, 950 F.2d 505 (8th Cir. 1991), the court held that when "a law enforcement officer merely recommends investigation of a particular individual based on suspicions arising serendipitously from an illegal search, the causal connection is sufficiently attenuated so as to purge the later investigation of any taint from the original illegality." *Id*. at 508. The court then concluded that the grand jury's use of the defendant's name and alias did not taint a later investigation, despite the court assuming *arguendo* the illegality of the prior search that uncovered records containing the defendant's identifying

information. *See id*.; *see also Hoonsilapa v. INS*, 575 F.2d 735, 738 (9th Cir. 1978) ("[T]he mere fact that [a] Fourth Amendment illegality directs attention to a particular suspect does not require exclusion of evidence subsequently unearthed from independent sources." (citation omitted).

The circumstances here even more strongly compel finding attenuation than in the above cases because the law enforcement database search revealed only the slimmest of leads: the 818 number. HSI thus was required to take an additional investigative step just to find a name associated with the 818 number, as compared to the typical "unlawful lead" case in which the defendant's full identify is discovered through the illegal search or seizure. In addition, HSI acted lawfully by subpoenaing Google for information about the owner of the 818 number, and HSI's four month investigation between obtaining the 818 number and conducting the forensic laptop examination primarily involved the use of information in TECS that existed before the initial database search, which further shows that the 818 number, at most, "tipped off the [G]overnment … to the probable identity of the perpetrator." *United States v. Smith*, 155 F.3d 1051, 1063 (9th Cir. 1998); *cf. United States v. Crews*, 445 U.S. 463, 475 (1980) ("The exclusionary rule … does not reach backward to taint information that was in official hands prior to any illegality."). Accordingly, the Court concludes 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 that evidence.

c. Purpose And Flagrancy Of The Illegal Conduct

Lastly, the Court considers the "purpose" and "flagrancy" of the illegal law enforcement conduct. *See 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." *United States v. Washington*, 387 F.3d 1060, 1075 (9th Cir. 2004) (citation omitted); *see also Davis v. United States*, 131 S. Ct. 2419, 2427 (2011) ("When the police exhibit 'deliberate,' 'reckless, or 'grossly negligent' disregard for Fourth Amendment rights, the benefits of exclusion tend to outweigh the costs." (citation omitted)). In contrast, when law enforcement officials acted with an "objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrent value of suppression is diminished, and exclusion cannot 'pay its way.'" *Davis*, 131 S. Ct. at 2427 (citations omitted); *see also, e.g.*, *United States v. Boone*, 62 F.3d 323, 325 (10th Cir. 1995) (noting that "a mistaken belief" that the defendant "had consented to the search … rises to the level of a Fourth Amendment violation, [but] it does not qualify as flagrant misconduct that would tilt the scales against attenuation"); *United States v. Ramos*, 42 F.3d 1160, 1164 (8th Cir. 1994) (holding that attenuation existed when, among other considerations, the "officer's conduct was in good faith" and "not flagrant"); *United States v. Richard*, 994 F.2d 244, 252 (5th Cir. 1993) (holding that attenuation existed when, among other considerations, "both agents reasonably believed that they had consent to search" defendant's motel room).

The Court, however, is left slightly in the dark regarding the flagrancy element because the Government has strategically refused to provide details about the law enforcement database it used. Based on the Government's affidavits and briefing on the motion to suppress, the Court knows only that the database was accessible to HSI and that this database was not the NSA program discussed in *Klayman*. The Court may surmise, though, that the law enforcement database operates fairly similarly to the NSA program, at least insofar as the database also appears to include a repository of aggregated telephone records for calls made into the U.S. from

abroad. *Cf. Klayman*, 957 F. Supp. 2d at *14-19 (describing the NSA's bulk telephony program). The Court can reach this conclusion because HSI used the database to search retrospectively for telephone calls between Sheikhi's Iranian telephone number and any U.S. number, which suggests that the database includes, at a minimum, a collection of past telephone calls from foreign numbers into the U.S.

Such ambiguity, however, leaves the Court in a difficult position. For example, if the Court treats the HSI law enforcement database as functionally equivalent to the NSA telephony program, the Court likely would conclude that HSI acted in good faith because federal courts generally have approved of the NSA program, with the exception being Judge Leon's opinion in *Klayman*, which itself is on appeal before the D.C. Circuit. *See* Gov't's Mem. Opp'n Mot. Suppress 19 n.5 (citing cases upholding the NSA program). Further, even if the Court accepts *Klayman* as the authoritative statement on the NSA program's legality, *Klayman* was not decided until 2013, while the HSI database search occurred in 2011, at which time it appears that no federal court had deemed the program unconstitutional. *See Davis*, 131 S. Ct. at 2429 ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule.").

But, at the same time, the Court does 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. In particular, the NSA program was specifically limited to being used for counterterrorism purposes, *see Klayman*, 957 F. Supp. 2d at 15-16, and it remains unclear if the database that HSI searched imposed a similar counterterrorism requirement. If 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 terrorism activities. With so many caveats, the Government's litigation posture leaves the Court in a difficult, and frustrating, situation. Yet, 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.[6] *Cf. Carter*, 573 F.3d at 421 (admitting evidence after illegal search of defendant's residence); *Smith*, 155 F.3d at 1059 (admitting evidence resulting from an "illegally intercepted wire communication"); *Friedland*, 441 F.2d at 856 (admitting evidence after the "FBI unlawfully installed electronic 'bugs'" in an office).

The Court is more certain, though, that HSI did not search the law enforcement database for the purpose of "extracting evidence against the defendant." *Washington*, 387 F.3d at 1075 (citation omitted). When it executed the database search using Sheikhi's business telephone number, HSI had no inclination that Hassanshahi was involved with Sheikhi or his company; indeed, the agency used the law enforcement database to cast a wide net for potential U.S.-based suspects for the very reason that it had no leads into U.S. suspects at the time. Thus, although that net eventually ensnared Hassanshahi, the lack of initial targeting compels the Court to conclude that HSI did not act purposefully or in bad faith to violate Hassanshahi's constitutional rights.

[6] The Government's silence regarding the nature of the law enforcement database has made the Court's analysis more complex than it should be. Although the Court still concludes that the attenuation exception applies in large part based on the "unlawful lead" line of cases, the Court will order that the Government provide the Court with an *ex parte* declaration summarizing the contours of the mysterious law enforcement database used by HSI, including any limitations on how and when the database may be used.

4. *United States v. Scios* and *United States v. Najjar* Do Not Compel A Different Result

Finally, the Court must address two arguments raised through Hassanshahi's reply memorandum. First, Hassanshahi argues that the D.C. Circuit's *en banc* decision in *United States v. Scios*, 590 F.2d 956 (D.C. Cir. 1978), is directly on point and compels against finding attenuation. *See* Def.'s Reply Supp. Mot. Suppress 20-19. In *Scios*, law enforcement agents illegally searched sixty file folders located in the defendant's home after the defendant had been arrested. *See id*. at 958. One of the folders contained various papers, including a credit card receipt for a motel bearing the defendant's name and an itemized bill from the same motel indicating that "Mr. Massa" had registered for the room. *See id*. The agents issued a subpoena to require Massa to appear before a grand jury regarding the defendant's possible unlawful activity, namely wiretapping. *See id*. Massa initially refused to testify, but he later agreed after the prosecutor granted him immunity and threatened contempt for any further refusal. *See id*. at 958-59. After the defendant was indicted, he moved to suppress Massa's testimony as fruit of the illegal seizure of the credit card receipt. *See id*. at 959. The *en banc* court held that Massa's testimony was inadmissible because his decision to testify was "made solely to avoid being jailed for contempt." *Id*. at 961. The court also noted that the taint from the illegal search had not dissipated because the agents were unaware of Massa's existence prior to the search, and because Massa agreed to testify only in response to official pressure, not through his own volition. *Id*. at 963-64.

The Court finds that *Scios* is inapplicable to the instant case. *Scios* involved applying the fruit of the poisonous tree doctrine to testimony from a witness whose identity was uncovered through a search that violated the defendant's Fourth Amendment rights. Thus, in *Scios*, and in other cases relying on *Scios* since then, the question was whether a witness voluntarily had

chosen to testify such that the testimony may be considered attenuated from the prior unlawful search. *See Scios*, 590 F.2d at 960 ("In certain circumstances, the attenuation doctrine has been applied where the witness who has been located as the result of an illegal search or seizure has voluntarily decided to testify." (citations omitted)); *id*. ("Turning to the case before us, we examine first the claim that the taint of the illegal seizure was attenuated by a voluntary decision to testify."); *see also United States v. Stevens*, 612 F.2d 1226, 1230 (10th Cir. 1979) (comparing *Scios* and affirming the district court's decision to admit witness testimony when the witness "offered to testify" in part due to "a desire 'to change his life-style and stay out of trouble,'" not due to the threat of contempt or other penalties like in *Scios*); *United States v. Davis*, No. CRIM. 10-339, 2011 WL 1655549, at *5-6 (D. Or. May 2, 2011) (comparing *Scios* and admitting witness testimony when the witness "made an independent and voluntary decision to speak with the officers several months after she was identified as a result of an illegal search," such that attenuation existed).

Here, there is no witness testimony against Hassanshahi, and even stretching *Scios* to its plausible limits, Hassanshahi has not, and cannot, demonstrate how any relevant physical evidence against him might be considered "coerced" like the witness in *Scios*. *Cf. Scios*, 590 F.2d at 961 ("[I]t is plain that Massa's giving of testimony before the grand jury, and presumably at the trial is purely and simply a product of coercion."). Instead, the unlawful law enforcement database search allowed HSI to uncover the identity of Hassanshahi — the *defendant*, not a witness and not evidence in and of itself — by linking him to the 818 number through the Google subpoena; the 818 number then led HSI to other *physical* evidence, such as that in TECS, not any witness testimony. Accordingly, the scenario here is both factually and legally distinct from *Scios*. The correct analysis, in fact, involves the "wrongful lead" cases, discussed above, in

which a limited piece of illegally obtained evidence directs law enforcement to focus its subsequent lawful investigation on the defendant, not on involuntary witness testimony cases like *Scios*.[7]

Second, Hassanshahi suggests through his reply memorandum that *United States v. Najjar*, 300 F.3d 466 (4th Cir. 2002), requires the Court to find a lack of attenuation here. *See* Def.'s Reply Supp. Mot. Suppress 23-25. Not so. In *Najjar*, the defendant argued that the district court erred by admitting evidence obtained through two search warrants when much of the evidence used to obtain those two warrants came from the execution of an earlier warrant in 1995 that later was invalidated. *See id.* at 475. In affirming the district court's decision, the Fourth Circuit explained that the officer's "investigation was not a simple matter of looking at salvage certificates obtained in the 1995 search and obtaining new evidence from their use, rather it was a substantial investigative effort unconnected to the seized documents themselves[.]" *Id*. at 479. The court then relied on a theory similar to the "wrongful lead" doctrine by explaining that "it is not enough that the original certificates may have triggered [the officer's] suspicion or gave impetus or direction toward what is to be focused on by the government." *Id.* (internal citation and quotation omitted). Thus, the court concluded that "[e]ven if the original illegal search in some slight way was a but-for cause of the later searches,

[7] Even ignoring this fundamental difference, *Scios* still does not compel a different result here. There is no doubt that in the case of both Messa's testimony in *Scios* and the forensic examination of Hassanshahi's laptop, "but for" the initial unlawful search, law enforcement would not have uncovered the relevant evidence, thus making both pieces of evidence "fruit" of the poisonous tree. *Cf*. Def.'s Reply Supp. Mot. Suppress 22 (arguing that "[j]ust like Massa's testimony in *Scios*, the computer search in this case is fruit of the poisonous tree and should be suppressed"). But unlike in *Scios*, where the D.C. Circuit found no attenuation primarily due to a lack of voluntariness by Messa, all three attenuation factors in this case suggest that the illegal taint from the database search was purged by the time of the forensic examination. Hassanshahi fails to appreciate that merely having "but-for" causation does not require suppression when other attenuating factors are at play.

[the officer's] two-year investigation and the intervening circumstances were sufficient to break the causal link between any primary illegality and later obtained evidence." *Id*.

Though HSI's investigation into Hassanshahi lasted several months rather than two years, the conclusion in *Najjar* in consistent with the Court's decision here because of the significant investigative steps HSI took between the database search and the forensic examination, as well as the limited probative value of the unlawfully discovered 818 number. To distinguish the cases, Hassanshahi asserts that "no time at all passed between the illegal search (accessing the telephony database) and when the agent ordered the computer search when and if Hassanshahi returned to the U[.]S." Def.'s Reply Supp. Mot. Suppress 25. But Hassanshahi's argument misstates the facts of the case and therefore focuses on the wrong timeframe. In reality, the HSI agent did not order the forensic examination "when and if Hassanshahi returned to the U[.]S." *Id*. Instead, on November 29, 2011, the agent "augmented the existing TECS records regarding Hassanshahi by entering instructions that [the agent] should be alerted if and when [Hassanshahi] returned to the United States, and that [Hassanshahi] should be referred for secondary screening by [CBP] officers when he returned to the U.S." 2d Akronowitz Aff. ¶ 17. There is no support in the record for Hassanshahi's claim that the forensic examination also was ordered on November 29 or, for that matter, at any other time prior to Hassanshahi's arrival at LAX on January 12, 2012. Indeed, the record does not reflect any evidence that law enforcement had any way of knowing which devices, if any, Hassanshahi would possess when he eventually crossed the border at a then-unknown date.

Alternatively, even if the Court used November 29, 2011, as the relevant date, most of the key investigative steps leading to the forensic examination already had occurred between then and the August 24, 2011, database search such that the same temporal proximity analysis

should apply. Thus, Hassanshahi's suggestion that "[t]here was no time for any independent investigation" during this two month period, *see* Def.'s Reply Supp. Mot. Suppress 25, is not supported by the undisputed facts in the record, which show that HSI did conduct an independent investigation in this period by using, for example, TECS and a Google subpoena.[8] Lastly, Hassanshahi asserts that *Najjar* is distinguishable because the circuit court there agreed with the district court's finding that the original violation was not purposeful or flagrant. *See id*. As this Court has explained, however, it reaches the same conclusion as *Najjar* about the lack of purposefulness or flagrancy with regard to the database search. Simply put, then, nothing in *Najjar* requires a different conclusion here.[9]

* * *

In sum, the Court finds that all three attenuation factors compel in favor of finding that the initial taint of illegality from the law enforcement database search was purged. Accordingly, the Court concludes that the "causal chain" leading to the discovery of laptop evidence was "too attenuated to justify exclusion." *Brodie*, 742 F.3d at 1063 (citation and quotation omitted). The Court therefore refuses to suppress the laptop evidence on this basis.

---

[8] Hassanshahi also argues that "there was no independent source of information" linking Hassanshahi to Sheikhi. *See* Def.'s Reply Supp. Mot. Suppress 25. Though true that the database search provided the only link between Hassanshahi and Sheikhi, Hassanshahi does not explain why this fact is relevant to the attenuation analysis.

[9] It appears to the Court that Hassanshahi actually may be arguing about the independent discovery exception to the fruit of the poisonous tree doctrine, not attenuation. *Cf. United States v. Holmes*, 505 F.3d 1288, 1293 (D.C. Cir. 2007) (explaining that inevitable discovery, discovery through independent means, and attenuation are alternative methods for dissipating the taint from an unlawful search or seizure). If that is the case, Hassanshahi presents a straw man argument because the Government never suggested that it discovered the laptop evidence through independent means.

C. Reasonable Suspicion Existed For The Forensic Laptop Examination

The broad power of the Government to conduct searches at the international borders is rooted in "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country."[10] *United States v. Ramsey*, 431 U.S. 606, 621 (1977). The Supreme Court therefore has explained that "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). Given the strong interests at stake, the Supreme Court has "[t]ime and again … stated that 'searches made at the border … are reasonable simply by virtue of the fact that they occur at the border.'" *Id*. at 152-53 (quoting *Ramsey*, 431 U.S. at 616).

Notwithstanding this sweeping language about the Government's expansive border search power, the Supreme Court has suggested over the years that the Fourth Amendment may impose some limits even at the nation's borders, though the Court has not always spoken definitively on that subject, nor has it clearly defined such limits, if any. *Cf. Flores-Montano*, 541 U.S. at 152-53, 155-56 (noting that there are "reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person-dignity and privacy interests of the person being searched," as well as in the case of searches of property that are "destructive"); *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 & n.4 (1985) (noting that the Court has "not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search"); *Ramsey*, 431 U.S. at 618 n.13 (leaving open the question of "whether, and under what circumstances, a border search

[10] As a threshold issue, it is well settled that searches of passengers on incoming international flights at a U.S. airport are considered the "functional equivalent of a border search" for Fourth Amendment purposes. *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973).

might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out"). Indeed, "the ultimate touchstone of the Fourth Amendment is 'reasonableness,'" *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006), so it appears only logical that some circumstance might arise at the border when the Government's conduct nudges into unreasonableness territory.

Hassanshahi now argues that this Court should recognize one such limit to the border search power by following two recent federal court decisions — *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), and *United States v. Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014) — and holding that the Fourth Amendment required reasonable suspicion to conduct the forensic examination of Hassanshahi's laptop following the border stop. Before reaching the legal merits of this position, however, the Court first must determine whether reasonable suspicion did in fact exist. And because the Court ultimately concludes that there was reasonable suspicion for the forensic examination of Hassanshahi's laptop, the constitutional question of whether that examination required reasonable suspicion becomes moot.[11]

[11] Interestingly, both *Cotterman*, 709 F.3d at 970 ("[W]e conclude that the examination of Cotterman's electronic devices was supported by reasonable suspicion and that the scope and manner of the search were reasonable under the Fourth Amendment."), and *Saboonchi*, 990 F. Supp. 2d at 571 ("All of this is more than sufficient to give rise to reasonable, particularized suspicion — if not probable cause — that Saboonchi was involved in violations of export restrictions on Iran."), found reasonable suspicion for the respective forensic computer examinations, yet both courts spent considerable space addressing a constitutional question that had no practical effect on the final disposition of the case. By contrast, this Court finds that engaging in such an exercise would be imprudent unless reasonable suspicion was found not to exist. *See Stillman v. CIA*, 319 F.3d 546, 548 (D.C. Cir. 2003) (holding that the district court abused its discretion by "unnecessarily" deciding a First Amendment question and explaining that "'[a] fundamental and longstanding principle of judicial restraint requires that courts avoid reaching constitutional questions in advance of the necessity of deciding them.'" (quoting *Lyng v. Nw. Indian Cemetery Protective Ass'n*, 485 U.S. 439, 445 (1988)).

1. Reasonable Suspicion Standard

Reasonable suspicion exists when a law enforcement officer has "specific and articulable facts," which, considered together with rational inferences from those facts, indicate that criminal activity "may be afoot." *Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968). When making the reasonable suspicion determination, courts are instructed to view the "totality of the circumstances" and not engage in a "divide-and-conquer analysis" in which courts consider whether each fact is "susceptible to an innocent explanation." *United States v. Arvizu*, 534 U.S. 266, 274 (2002). Thus, "[a] determination that reasonable suspicion exists … need not rule out the possibility of innocent conduct." *Id*. at 274 (citation omitted).

In addition, officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that 'might well elude an untrained person.'" *Id*. at 273 (quoting *United States v. Cortez*, 449 U.S. 411, 418 (1981)); *see also Ornelas v. United States*, 517 U.S. 690, 699 (1996) (reviewing court must give "due weight" to factual inferences drawn by law enforcement officers). Though an officer's reliance on a mere "inchoate and unparticularized suspicion or 'hunch'" is insufficient to establish reasonable suspicion, *see Terry*, 392 U.S. at 27, the likelihood of criminal activity need not rise to the level required for probable cause, nor even to the preponderance of the evidence standard. *See United States v. Sokolow*, 490 U.S. 1, 7 (1989).

Before turning to the reasonable suspicion analysis, the Court notes that it must exclude from the calculus evidence of the one telephone call between Sheikhi's business phone number and Hassanshahi's 818 number because this evidence was the clear and direct result of an unconstitutional search, as conceded by the Government. *See, e.g.*, *United States v. Karo*, 468 U.S. 705, 719 (1984) (explaining that "if sufficient untainted evidence was presented in the

warrant affidavit to establish probable cause, the warrant was nevertheless valid" (citation omitted)); *United States v. Pina-Aboite*, 109 F. App'x 227, 234 (10th Cir. 2004) (explaining that because the officer violated the Fourth Amendment by extending the scope of a traffic stop after finding no traffic violation, incriminating statements made later during the stop were tainted and could not contribute retrospectively to establishing reasonable suspicion for the prolonged stop); *United States v. Eustaquio*, 198 F.3d 1068, 1071-72 (8th Cir. 1999) ("As the touching of the defendant's midriff area was violative of the Fourth Amendment, any evidence resulting therefrom is inadmissible and cannot be used to determine whether there was a reasonable suspicion to detain or search her."). The Court next turns to the remaining evidence known about Hassanshahi prior to the forensic examination.

2. Hassanshahi's Criminal History And Frequent Travel To Iran

Prior to conducting the forensic examination, HSI conducted research on Hassanshahi in TECS, which led HSI to discover details about a 2003 federal investigation into Hassanshahi's participation in a conspiracy to establish an American company for the purpose of entering into an agreement with a Chinese company to build a computer production facility in Iran.[12] Federal

[12] In his reply memorandum, Hassanshahi suggests that the probative value of the 2003 HSI investigation is significantly lessened because he was "cleared" of any criminal misconduct. The decision not to file criminal charges, however, does not automatically equate to him having been cleared of all wrongdoing, and anyway, it is the facts uncovered about Hassanshahi's role in the scheme to violate the Iran export embargo that are probative of a potential new scheme to violate the same laws in 2011, not the ultimate decision not to file charges. Indeed, according to the California state court decision dismissing Hassanshahi's breach of contract claim as against public policy, Hassanshahi and his co-plaintiffs specifically alleged that "they and defendants [Chinese companies] agreed to establish an Iranian corporation to manufacture notebook computers in [Iran's] free trade zone and to sell that product in Iran and in neighboring countries." *Kashani v. Tsann Kuen China Enter. Co.*, 118 Cal. App. 4th 531, 537-38 (Cal. App. 2d Dist. 2004). Plaintiffs also alleged that as part of this agreement, they "traveled to Iran to begin setting up the plant," "secured the necessary governmental cooperation," and "invested considerable funds, time and resources into the project to find the land, plan the facility, and other expensive preparations … [and to] make certain commitments,

circuit courts have consistently held, however, that a person's criminal history is insufficient to create reasonable suspicion by itself. *See, e.g., United States v. Johnson*, 482 F. App'x 137, 148 (6th Cir. 2012) ("The fact that [defendant] had committed crimes in the past, while it has a place in the reasonable-suspicion analysis, is not, without more, strong evidence of criminal activity in the present."); *United States v. Walden*, 146 F.3d 487, 490 (7th Cir. 1998) ("Reasonable suspicion of criminal activity cannot be based solely on a person's prior criminal record."). But, at the same time, "criminal history contributes powerfully to the reasonable suspicion calculus," *United States v. Santos*, 403 F.3d 1120, 1132 (10th Cir. 2005), and an officer's "knowledge of the individual's criminal history help[s] to dispel any likelihood that the observed conduct actually was innocent." *United States v. Monteiro*, 447 F.3d 39, 47 (1st Cir. 2006).

Here, HSI's 2003 investigation into Hassanshahi's scheme to violate the Iran trade embargo was relevant for more than just establishing Hassanshahi's general history with law enforcement, as his past activity in Iran also negatively colored the perception of any future travel by him to that specific country. Thus, Hassanshahi's travel to Iran after 2003 should not be measured as general travel abroad to a foreign country like another person's travel might, but rather as him returning to the specific "scene of the crime," for lack of a better term. Travel to Iran, then, becomes a particularized and objective fact potentially indicative of ongoing criminal activity by Hassanshahi because one quite reasonable explanation for his ongoing presence in Iran was that he continued to conduct business involving that country, similar to what he did in 2003. *Cf. Reid v. Georgia*, 448 U.S. 438, 440-41 (1980) (finding no reasonable suspicion in large part because defendant's arrival "from Fort Lauderdale, which the agent testified is a

---

including [with] the government [of Iran]." *Id*. at 548 (internal citations and quotation marks omitted). Given Hassanshahi's own admissions in the civil lawsuit, the assertion that no criminal charges were filed may be true, but that does not negate the reality of the underlying events.

principal place of origin of cocaine sold elsewhere in the country[,] … describe[d] a very large category of presumably innocent travelers, who would be subject to virtually random seizures were the Court to conclude that as little foundation as there was in this case could justify a seizure."); *Cotterman*, 709 F.3d at 992 (Smith, J., dissenting) (criticizing the majority for finding reasonable suspicion based in large part on defendant recently traveling to Mexico, a country broadly associated with "sex tourism," because using such a generic fact to support reasonable suspicion potentially means that "thousands of individuals — many with decades-old convictions — will now be forced to reconsider traveling to entire countries or even continents, or will need to leave all their electronic equipment behind, to avoid arousing a 'reasonable' suspicion.").

In addition, TECS revealed not only that Hassanshahi was in Iran for some period of time between late 2011 and early 2012, but also that he had returned from Iran in 2006, twice in 2008, once in 2010, and once again in May 2011. Given Hassanshahi's history in acting to violate the Iran trade embargo, these frequent trips potentially were suggestive of a continuous illegal business relationship with someone in Iran, or with the country's government itself. *Cf. United States v. Glover*, 353 F. App'x 314, 317 (11th Cir. 2009) (finding that defendant's multiple "trips to Trinidad, which was known to be a high drug trafficking location," were indicative of drug smuggling and helped support reasonable suspicion); *Hurn v. United States*, 221 F. Supp. 2d 493, 503 (D.N.J. 2002) (finding that defendant's "repeated, prior trips to Jamaica," a "known drug source country," were indicative of drug smuggling and helped support reasonable suspicion); *United States v. Clymore*, 515 F. Supp. 1361, 1367 (E.D.N.Y. 1981) (evidence that defendant was returning from a trip to Pakistan, a country known as a source of narcotics; that defendant had made a number of other trips to the Middle East; and that defendant previously

had been arrested for attempted smuggling supported finding reasonable suspicion to conduct invasive strip search at airport).

This possibility was reinforced by the fact that in 2005, Hassanshahi was stopped, questioned, and then released by CBP officers after he returned from Dubai with $15,000 in cash, an act that also might suggest continued business activity in the Middle East following the 2003 investigation. Further, when Hassanshahi landed at LAX on January 12, 2012, he had approximately $7,000 in cash in his possession. *Cf. United States v. Chandler*, 437 F. App'x 420, 428 (6th Cir. 2011) (noting that "while the mere possession of currency is innocent behavior, the *large amount* of currency possessed by [defendant] was unusual" and indicative of a recent narcotics transaction) (emphasis in original); *United States v. Green*, 599 F.3d 360, 376 (4th Cir. 2010) (holding that the incriminating nature of a large sum of money could be "immediately inferred" when defendant was suspected of drug-related activities); *United States v. Whitney*, 391 F. App'x 277, 279, 282 (4th Cir. 2010) (discovery of roughly $3,000 in cash in defendant's pockets during a traffic stop was an important fact for justifying reasonable suspicion); *United States v. Chhien*, 266 F.3d 1, 8-9 (1st Cir. 2001) (discovery of $2,000 in cash during a traffic stop helped support determination of reasonable suspicion and justified a brief period of further detention); *Conrod v. Davis*, 120 F.3d 92, 97-98 (8th Cir. 1997) (discovery of $6,000 in cash in individual's pocket and $4,000 in suitcase helped establish reasonable suspicion). Together, these events further add to the pile of evidence known to HSI which suggested that Hassanshahi had maintained ongoing business dealings in the Middle East, and Iran in particular.

3. Accessing E-Mail Account In Iran And Telephone Calls From Iran

HSI also understood that Hassanshahi's e-mail account was accessed twenty-four times from an Iran IP address between December 8, 2011, and December 15, 2011. At the same time, however, this account was accessed from IP addresses in multiple other countries within minutes of apparently being accessed in Iran, which may suggest that other users had access to the account. Nonetheless, a "determination that reasonable suspicion exists … need not rule out the possibility of innocent conduct," *Arvizu*, 534 U.S. at 277, and Hassanshahi's seemingly frequent use of e-mail while in Iran suggests that he may have been conducting business while traveling to that country, especially in light of the 2003 investigation.

In addition, HSI possessed evidence that around the same time Hassanshahi traveled to Iran, he also made contact with one Iranian telephone number and received a missed call from another Iranian number. Though it certainly is possible that these two telephone calls were nothing more than innocent conduct by Hassanshahi, it also is plausible that the calls further indicated Hassanshahi's continued involvement in prohibited activities inside Iran. Again, as the Supreme Court and the D.C. Circuit have explained, "that an individual's conduct is 'ambiguous and susceptible of an innocent explanation' does not mean that it may not be grounds for suspicion: '*Terry* recognized that … officers could detain [such] individuals to resolve the ambiguity.'" *United States v. Brown*, 334 F.3d 1161, 1168 (D.C. Cir. 2003) (quoting *Illinois v. Wardlow*, 528 U.S. 119, 125-26 (2000)) (alteration in *Brown*).

4. Possession Of Multiple Electronic Devices At LAX

Finally, one additional fact weighs in favor of reasonable suspicion existing before the forensic laptop examination. When Hassanshahi landed at LAX, he possessed multiple electronic devices and data storage accessories, including a laptop computer, multimedia cards,

thumb drives, a camcorder, SIM cards, and a cell phone. *See* 1st Arkonowitz Aff. ¶ 19. Though it generally is unremarkable nowadays for a person traveling abroad to bring a computer, camcorder, or cell phone with them, Hassanshahi's possession of multiple data storage devices appears to be inconsistent with just personal use while traveling. Instead, one reasonable inference was that these data storage devices, and thus perhaps the corresponding electronic devices as well, were necessary for conducting business while Hassanshahi was in Iran. This inference then further supports the possibility that Hassanshahi traveled to Iran to engage in the same type of business activity for which he was investigated in 2003.

5. Totality Of The Circumstances And Reasonable Suspicion

Judicial review of the Government's argument for reasonable suspicion is "not a rubber stamp." *United States v. Freeman*, 735 F.3d 92, 103 (2d Cir. 2013). At the same time, however, the Court is mindful that reasonable suspicion sets a "low threshold," *United States v. Rivera*, 353 F.App'x 535, 537 (2d Cir. 2009), and requires only a "'minimal level of objective justification.'" *United States v. Edmonds*, 240 F.3d 55, 59 (D.C. Cir. 2001) (quoting *INS v. Delgado*, 466 U.S. 210, 217 (1984)). Further, though the contemporaneous evidence against Hassanshahi was, in a vacuum, innocent — travel to Iran; telephone calls from and e-mail activity in Iran; possession of legal electronic and data storage devices while traveling abroad — "the question of whether reasonable suspicion existed can only be answered by considering the totality of the circumstances as the officer on the scene experienced them." *Id.* at 59-60 (citations omitted). Indeed, "[a]n officer's training and experiences enable him to 'draw[] inferences and make[] deductions' from seemingly innocuous facts — 'inferences and deductions that might well elude an untrained person.'" *Id*. at 60 (quoting *Cortez*, 449 U.S. at 418) (alteration in *Edmonds*).

Here, HSI Special Agent Arkonowitz, who was in communication with the CBP officers who detained Hassanshahi at LAX, had several years of experience working for HSI, including specific experience with criminal investigations into the illegal exportation of goods from the U.S to Iran. *See* 1st Arkonowitz Aff. ¶ 1; 2d Arkonowitz Aff. ¶ 1. The Court also must consider the innocuous facts known about Hassanshahi not only for what they suggest taken together, but also for what they suggest in the context of the 2003 HSI criminal investigation. This investigation established a clear precedent of Hassanshahi attempting to violate the Iran trade embargo, and such evidence "contributes powerfully to the reasonable suspicion calculus." *Santos*, 403 F.3d at 1132. Indeed, as one circuit court has explained, law enforcement's "knowledge of the individual's criminal history" can "help[] to dispel any likelihood that the observed conduct actually was innocent." *Monteiro*, 447 F.3d at 47.

Ultimately, based on Hassanshahi's recent contacts with Iran — including the latest trip to Iran following a series of other visits to Iran in the past few years and the recent telephone calls from Iran — the large quantity of electronic devices and cash in Hassanshahi's possession when he returned from Iran in January 2012, and the 2003 criminal investigation into what may have been similar illegal conduct, the Court finds that law enforcement possessed "specific and articulable facts," which, considered together with rational inferences from those facts, indicated that Hassanshahi may have been up to his old tricks by again conducting business in violation of the Iran trade embargo. *See Terry*, 392 U.S. at 21; *see also* Wayne R. LeFave et al., Criminal Procedure § 3.8 (5th ed. 2009) ("The *Terry* reference to when 'criminal activity *may be* afoot' strongly suggests that though the arrest standard may sometimes require that guilt be more probable than not, this is never the case as to a stopping for investigation, where the very purpose is to clarify an ambiguous situation." (footnote omitted; emphasis in original)).

Other cases in which federal courts have found reasonable suspicion based on similar or lesser evidence are instructive. For example, in *United States v. Massi*, 761 F.3d 512 (5th Cir. 2014), the circuit court affirmed the district court's finding of reasonable suspicion to justify an investigatory inspection of an airplane based on the following: the plane's "suspicious" flight path and frequent refueling stops between Orlando and Las Vegas; the registered owner of the plane having been convicted of drug trafficking approximately twenty years prior; and a passenger on the plane having recently crossed from Tijuana, Mexico, "a known hub of the illegal drug trade," into the U.S. *See id*. at 518, 522-23. Similarly here, Hassanshahi had a history of illegal conduct directly relevant to the crime for which he now was suspected. In addition, Hassanshahi had recently traveled to Iran, a suspicious country that might be considered the "hub" of his illegal activity given the 2003 investigation, and he also had made multiple trips to Iran in recent years, which together could be considered a suspicious travel history given that Iran is not a common destination for U.S. citizens.

As another example, the district court in *United States v. Bunty*, 617 F. Supp. 2d 359 (E.D. Pa. 2008), considered the defendant's motion to suppress evidence that was found on his computer equipment during a search after he arrived at a Philadelphia airport on a flight from London. *See id*. at 363-64. After concluding that reasonable suspicion was not required for the search, the district court went on to consider whether such suspicion existed anyway. *See id*. at 365. In doing so, the court found that reasonable suspicion did exist for the computer search based on the following: the defendant had been arrested for the sexual abuse of a child and recently had pled guilty to corrupting the morals of a minor in that case; the defendant possessed a letter from his probation officer giving him permission to travel to England; the defendant possessed two laptop computers, a digital camera, a cell phone, and a variety of electronic

storage devices, including several compact discs, movie DVDs, flash drives, and floppy disks that could not be used with his computers; and the defendant had a history of "extensive international travel."[13] *See id*.

Similarly here, Hassanshahi had a criminal history relevant to the crime for which he now was suspected — there, possession of child pornography; here, violating the Iran trade embargo. In addition, Hassanshahi had recently traveled abroad, and he also had entered the U.S. with a variety of electronic devices and data storage accessories that could have been used in furtherance of the suspected illegal activity. Indeed, unlike the defendant in *Bunty*, who had just returned from London, which itself was not especially associated with criminal activity as to the defendant or in general, Hassanshahi had traveled to Iran, which was exactly where his prior relevant bad conduct had occurred.

Finally, in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013), a case on which Hassanshahi heavily relies, the Ninth Circuit's *en banc* majority found reasonable suspicion to conduct a forensic examination of the defendant's computer following a border stop at LAX based on the following: the defendant's 1992 conviction for child molestation; the defendant's recent travel to Mexico, a "country associated with sex tourism," as well as other unspecified recent travel outside the U.S.; the defendant's collection of electronic equipment at the border, which included the defendant and his wife each having a laptop and digital camera, as well as one video camera between them; and the existence of password-protected files on the defendant's computer. *See id*. at 968-70.

The Court finds that for several reasons, the facts supporting reasonable suspicion here are significantly more probative of ongoing criminal activity than the facts in *Cotterman*. First,

[13] It is unclear from the district court's opinion whether this travel referred to defendant's recent trip to England or other unknown international trips.

Hassanshahi's criminal history was only eight years-old at the time of the forensic examination, whereas Cotterman's conviction was fifteen-years old when the examination of his devices occurred. *See id*. at 957. Second, Cotterman's recent travel to Mexico, a "country associated with sex tourism," falls very close to the category of evidence that the Supreme Court has cautioned against using for reasonable suspicion because it "describe[s] a very large category of presumably innocent travelers," *Reid v. Georgia*, 448 U.S. 438, 441 (1980), while Hassanshahi traveled on multiple occasions to the specific country at issue in the 2003 criminal investigation, thus making his travel far more probative of criminal conduct.[14] Third, Cotterman and his wife each carried a laptop and digital camera when traveling to Mexico, as well as one video camera between them, which altogether does not appear particularly remarkable for international tourists. *Cf. Cotterman*, 709 F.3d at 992 (Smith, J., dissenting) ("In today's world, the fact that Cotterman and his wife each carried a laptop and digital camera when traveling internationally, as well as one video camera between them, is no more evidence of 'sex tourism' than of any other kind of tourism."). Hassanshahi, on the other hand, possessed a laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone, which together suggest a person engaged in business while traveling to Iran, not tourism. Finally, while the Ninth Circuit majority relied on Cotterman having password-protected files on his computer as the last fact supporting reasonable suspicion, several much more probative facts were known

[14] A more analogous situation would have been, for example, if Cotterman's 1992 conviction specifically involved child pornography that he had obtained from, or that perhaps had been made in, Mexico, which would have made his travel to Mexico more relevant and specific than just a visit to a country generically associated with certain criminal activity. *Cf. Cotterman*, 709 F.3d at 992 (Smith, J., dissenting) ("[T]he fact that Cotterman was returning from Mexico fails to support a finding of reasonable suspicion. Mexico is a popular travel destination for Californians, including those who travel to Mexico for its beaches, culture and weather, and not for its sex tourism. Travel to Mexico simply does not support reasonable suspicion without more specific evidence that Cotterman traveled to a particular establishment, city, or even region, associated with sex tourism.").

about Hassanshahi, such as the two recent telephone calls from Iran, the 2005 questioning by CBP officers after Hassanshahi returned from Dubai with $15,000 in cash, Hassanshahi's multiple other trips to Iran in recent years, and Hassanshahi's possession of $7,000 in cash when he arrived at LAX in January 2012.[15]

* * *

The D.C. Circuit has held that "even though a single factor might not itself be sufficiently probative of wrongdoing to give rise to a reasonable suspicion, the combination of several factors — especially when viewed through the eyes of an experienced officer — may." *Edmonds*, 240 F.3d at 60. That is exactly the case here. Through the combination of multiple factors, none of which individually constituted direct evidence of criminal activity but all of which were consistent with the scheme uncovered during the 2003 HSI investigation, the Court finds that reasonable suspicion existed to conduct the forensic examination of Hassanshahi's laptop. Having reached this conclusion, the Court need not address whether reasonable suspicion was required as a matter of law because that question is rendered moot.

IV. CONCLUSION

For the foregoing reasons, the motion to suppress is **denied**. An order consistent with this Memorandum Opinion is separately and contemporaneously issued.

---

[15] In his reply memorandum, Hassanshahi compares the facts known about him to the facts on which the district court found reasonable suspicion for a forensic examination in *Saboonchi*, 990 F. Supp. 2d 536 (D. Md. 2014). Without doubt, more information was known about Saboonchi than was known about Hassanshahi at the time of the respective forensic examinations. *Saboonchi*, however, does not set the floor of what evidence is required for reasonable suspicion, and in fact, the district court there indicated that the evidence may even have met the much higher probable cause threshold. *See id*. at 571 ("All of this is more than sufficient to give rise to reasonable, particularized suspicion — if not probable cause — that Saboonchi was involved in violations of export restrictions on Iran.").

Dated: December 1, 2014

RUDOLPH CONTRERAS
United States District Judge