SAIED KASHANI, pro had vice California SBN 144805
800 West First Street Suite 400
Los Angeles, California 90012
tel. (213) 625-4320
fax (213) 652-1900
email: **saiedkashani@gmail.com**

Attorneys for Defendant
SHANTIA HASSANSHAHI

UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	**CRIMINAL CASE 13-274-RC**
Plaintiff,	**DEFENDANT'S REPLY RE MOTION TO SUPPRESS EVIDENCE [FR Crim.P 12(b)(3)(C)]**
v.	
SHANTIA HASSANSHAHI,	**Hearing: November 3, 2014 10am**
Defendant.	

TABLE OF CONTENTS

TABLE OF AUTHORITIES

SUMMARY

1a. In response to the motion to suppress, government refuses to disclose ***any details whatsoever*** of the telephony database -- the direct, proximate, unavoidable and material basis of the "reasonable suspicion" supporting the forensic search of defendant's computer at Los Angeles International Airport in 2011. Contrary to government's belief, such a forensic search at LAX was not "free" but required "reasonable suspicion" under controlling Ninth Circuit law, United States v. Cotterman, 709 F.3d 952 (2013). The district court in Maryland also just confirmed, in a detailed, highly reasoned opinion, and in the same context (alleged Iran sanctions violation) that "reasonable suspicion" is required for a forensic computer border search. United States v. Saboonchi, 990 F. Supp. 2d 536 (D.Md. 2014).

1b. Govt tries to argue Cotterman is "wrong" and should just be ignored. Cotterman is controlling law where the search was actually conducted (Los Angeles) and controls this inquiry regardless of the govt's preferences. Moreover, Cotterman is fully consistent with the Supreme Court's recent decision in Riley v. California, 134 S.Ct. 2473 (2014). The Court there held found an enormous privacy interest in cell phones due to their capacity and use to store private information. The same considerations apply to defendant's computer -- indeed the Supreme Court noted that cell phones "are in fact minicomputers." Thus Cotterman is not only the law, it is fully consistent with Supreme Court precedent.

2. The failure to disclose any details of the database, alone, is tantamount to refusing to articulate grounds for reasonable suspicion and thus mandates suppression. The burden is on government to articulate *facts*, not hunches and theories, to support reasonable suspicion, for example for a "Terry" stop. U.S. v. Williams, 878 F. Supp. 2d 190, 197 (D.D.C. 2012). Government fails this burden when it refuses to disclose any details whatsoever regarding the telephony database. Refusal to disclose, where government has the burden, fails the test. If there is no reasonable suspicion for the stop/search, evidence acquired thereby or therefrom is tainted and inadmissible. U.S. v. Beck, 140 F.3d 1129, 1140 (8th Cir. 1998), citing Wong Sun v. United States, 371 U.S. 471, 484-86 (1963).

3. As a separate grounds for suppression, the database as described functions entirely like the NSA database whose use (government admits) is limited to terrorism, and which is likely unconstitutional. Government argues *in its memorandum* that the subject database is not the NSA database, but this information appears nowhere in evidence or in any affidavit. It is unsupported attorney argument and meaningless for purposes of this motion. The government refuses to produce the agent to clarify matters. In the absence of *evidence* to the contrary, the court is entitled to assume the subject database either is the NSA database or is a database that functions and is regulated the same as the NSA database. Its use in this non-terrorism context was thus unlawful and will not support reasonable suspicion for the forensic computer search. See, e.g., Beck, 140 F.3d at 1140 (evidence obtained from otherwise

lawful search in detention following unreasonable stop will be suppressed).

4a. There is no "inevitable discovery" through an independent lawful source or "attenuation" to purge the taint of the improperly obtained evidence. Neither the Austrian informant, nor the email from "Sheikhi" in Iran, nor the Google search on Sheikhi's email activity, yielded any information regarding defendant Hassanshahi or in any way mentioned Hassanshahi. The *sole* and *entire* basis was the database search, specifically, an inquiry of Sheikhi's telephone number in Iran which allegedly yielded an 818 number linked to Hassanshahi. Government had no knowledge of Hassanshahi *but for* the database search, which yielded the 818 number. *Only after* obtaining the 818 number from the database, the government subpoenaed Google and tied the 818 number to Hassanshahi, and then performed some limited investigation of Hassanshahi before ordering the LAX forensic computer search. (The scope of this post-database investigation is in doubt -- the agent has *materially* altered and enlarged his affidavit in this regard.) There was no "independent source" and no "attenuation" -- there is a direct, unbroken, proximate and unswerving chain from the database inquiry to the LAX search. There was no "inevitable discovery" -- the government would not have known of Hassanshahi at all, ever, but for the database. In such circumstances there is no saving theory and the evidence is suppressed.

4b. Where, as here, the evidence (results of the computer search) were "come at by exploitation of the primarily illegality" (the telephony database), the evidence will be

suppressed. Wong Sun, 371 US at 478. In this regard, govt ignores the controlling case directly on point and with similar facts, U.S. v. Scios, 590 F.2d 956 (D.C.Cir. *en banc* 1978). In Scios, agents, incident to an arrest, unlawfully opened and read a file folder which contained a *telephone number* that govt traced to a witness who provided evidence against the accused. This Circuit held *en banc* that because finding the witness was the result of a "straightforward exploration of leads in the file," the exclusionary rule applies. Identically here, the investigation began with a *telephone number* improperly obtained from the database, which led directly to the LAX computer search. The resulting evidence should be suppressed in this case as it was in Scios.

4c. Govt materially miscites the cases on "attenuation" and "inevitable discovery." In Friedland, the investigating officer testified he and his squad had never received any information from the unlawful wiretapping, i.e. there was no connection between the illegal search and the resulting conviction. Any commentary on "attenuation" was thus dicta. 441 F.3d 855, 857 (2nd Cir. 1971). In Najjar, a two-year independent investigation followed the initial unlawful search, and the unlawfully obtained documents were obtained from independent sources. 300 F.3d 466, 479 (4th Cir. 2002). Govt ignores the controlling case on point which is Scios.

4d. Govt claims the "subsequent crime" of crossing the border purges the taint of the unlawful search, but the only "crime" identified is entering the country at LAX. Crossing the border is not a crime. Hassanshahi was not carrying any

contraband and transport of the documents allegedly found on his computer, alone, was not a crime. (This differs from the usual border search case which involves child pornography, the mere possession or transport of which is itself a crime.)

5. Not least of all, the govt's agent Akronowitz has submitted three materially different affidavits, none of which are supported by the documents the government has produced. At a minimum this mandates taking evidence from the agent.

Affidavit No. 1, filed 2011 with original complaint: (a) Akronowitz claimed the Google subpoena related to the 818 affidavit showed "numerous phone calls between Hassanshahi's 818 number and one Iranian phone number." (b) Akronowitz made no mention of, and did not claim he conducted any TECS search in October 2011 that referenced that Hassanshahi had ever been investigated before.

Affidavit No. 2, filed 2012 with opposition to this motion: (a) Akronowitz continues to claim "numerous phone calls etc." (b) Akronowitz adds an entirely new paragraph 16, in which he claims he researched TECS in October 2011 and found reference to a prior investigation. This (b) appears nowhere in the original affidavit and was presumptively *not* a basis for the LAX computer search conducted in January 2012. More likely, this TECS search was conducted *after the fact*, indeed in response to the instant suppression motion. Note that the actual records of the TECS search (Bates 113) were printed 100114 i.e. October 1, 2014 and not in 2011.

Affidavit No. 3, filed October 14, 2014 just before the hearing: Akronowitz now admits there were not "numerous phone

calls" but only a *single* phone call between the 818 number and a number in Iran -- *not* the number of Sheikhi or of anyone else of interest. And this short call was drowned in a sea of calls to Los Angeles numbers in 818, 805, 310 etc. area codes. Akronowitz claims there was one other missed phone call to an Iranian cel number, but even this number, on the government's production (filed herewith at Bates 085), does not have the Iran country code of "98". Akronowitz changed his affidavit only after defendant sought and received the actual Google phone records.

All three Akronowitz affidavits also claimed a subpoena indicated Hassanshahi had accessed his gmail account "twenty-four times" "while located in Iran" from December 8-15, 2011. The actual data (government production at Bates 094-098) is meaningless. The data on its face indicates the account was accessed from Iran but also from the United States on the same day, sometimes within the same 10 minute period, and then again from the United States scores of times, and then alternately from Iran and from Germany during the same two-hour period. Unless this is a particularly mobile computer, this indicates either multiple people in multiple countries were accessing the same account at the same time (indicating some kind of public account not tied to Hassanshahi alone) or that the data itself is flawed. But Akronowitz makes no mention of this in his affidavit.

6. Even if the database search is allowed, the govt lacked reasonable suspicion for the LAX computer search. The only reasonable suspicion in this case was:

(a) A single alleged call between Sheikhi's office number and the 818 number linked to Hassanshahi: date, time and duration undisclosed, contents unknown, participants unknown.

(b) Hassanshahi telephoned a number in Iran not associated with the investigation, once (and not "numerous times") as originally claimed by the agent.

(c) Hassanshahi's gmail account may have been accessed from Iran at some point, but the data is completely unclear and supports no conclusions.

(d) Newly alleged knowledge of a prior investigation -- which took place, if at all, over a decade ago and resulted in no charges and not even an interview.

There was simply no evidence that a current crime was afoot as would constitute reasonable suspicion. Cotterman at 167.

By contrast, in Saboonchi, where the court did find sufficient reasonable suspicion for a forensic computer search, the govt had the following evidence *prior* to instigating the search:

(a) A Fedex airbill that showed that Saboonchi had in fact shipped a restricted device to a company in United Arab Emirates;

(b) Investigation of the UAE company showed it was linked to a company in Iran dealing in similar goods

(c) Interviews with the manufacturer of the goods that confirmed Saboonchi had purchased the goods and misrepresented their end user as "domestic"

(d) Airbill misrepresented the value of the goods.

All of this data was gathered before the computer search

and, the court held, constituted reasonable suspicion for the search of Saboonchi's computer. Govt here had nothing even approaching this level before instigating the forensic search of Mr. Hassanshahi's computer.

The government refuses to disclose material information which it has the burden to disclose. The affiant repeatedly changes his story, and his story does not bear scrutiny. The computer search was the result of an unlawful database and insufficient reasonable suspicion. The results of the search should be suppressed.

STATEMENT OF THE CASE

One fact remains through three materially different affidavits and all the government argument: the sole, unbroken and unattenuated link to the LAX computer search was the still-undisclosed government telephony database. The government exploited the database to derive the evidence at issue.

1. Despite apparently being offered or paid financial confirmation, the "Source" in Austria (a paid informant with every reason to repeat every name he every heard in his life -- see Govt Prodn at 005 -- never mentioned defendant Shantia Hassanshahi in any way, shape or form. He also never disclosed any 818 number and never talked to defendant, ever.

2. The "Source" instead gave agents an email the Source had received from "Sheikhi" of the "radyab" company in Iran. The email gives Sheikhi's telephone number in Iran as 982144406457. GP 008

3. Agent Akronowitz then researched radyab (affdavits para. 14). This research also did not yield any 818 number or

Hassanshahi.

4. Akronowitz then ran an inquiry on Sheikhi's telephone number from the email in a telephony database. This database yielded an 818 number. Government refuses to disclose any details whatsoever regarding the database. However, the following is clear:

(a) There was no subpoena on Hassanshahi's telecoms provider or any telecoms provider related to his telephone number. There could not have been, because the government did not have Hassanshahi's number or name.

(b) For the same reason, there was no pen register on Hassanshahi's number or even Sheikhi's number.

(c) The database must have been historic, comprehensive, retrospective and gathered from the telephone records of millions of Americans who had never and will never come under any suspicion. Otherwise, an inquiry with Sheikhi's number would not have yielded a telephone number previously allegedly called by Sheikhi. As held in Kayman, the comprehensive and historic nature of the database differentiates it from a pen register or even a subpoena of an identified individual's phone records.

5. Government had (or does not claim to have had) any information regarding either the *content* of the call from Sheikhi's number to 818 or even who was on the line.

6. There was, apparently, only a single call between the Sheikhi number and the 818 number. Hardly seems sufficient for a business transaction of any kind.

7. There was no *independent* or *untainted* source, ever, of

the 818 number or Hassanshahi's name. The government pursued Hassanshahi solely and proximately because of the database.

8. *Having obtained the 818 number from the database*, the government then immediately subpoenaed Google records to yield Hassanshahi's name associated with the 818 number. The government then subpoenaed Google phone records.

9. Here the agent's affidavit changes materially. In the first affidavit and in the second filed in opposition to this motion, the agent claims there were "numerous calls" from the 818 number to a "single" number in Iran. The agent even implies the "single" number in Iran was that of Sheikhi.

What is the truth? Only after defendant demanded and obtained the actual response to subpoena, the agent changed his story and admitted (third affidavit) there was only *one* call from the 818 number to a number in Iran. Moreover, this number was *not* that of Sheikhi or even related to Sheikhi.

The actual phone records show a sea of calls to numbers in 818, 805, 310, all Los Angeles telephone numbers, and only a single actual call to Iran. GP 080-090. The agent now claims a single missed call to Iran to "22932293", but this does not have a 98 country code thus is not Iran. GP 085. The number, with repeating digits, looks more like a dialing error. The agent would presumptively have seen this at the time and thus seen a person with minimal contact with Iran.

10. The agent also claims Hassanshahi's google account was accessed "repeatedly" from Iran. The reality is far less clear. The actual records (GP 094-098) appear to show access from a United States IP address (beginning with "108"), then from an

Iran IP address ("178"), followed by Germany (195), then Iran again, then US, alternating sometimes within the same few minutes. Unless this computer moved with the speed of light from country to country, the record actually suggests the account was accessed from multiple locations around the world at the same time. This indicates a public account, not an account confined to Hassanshahi. The agent would, again, have seen these records and should not have attributed the Google account to a single person (this also has implications for emails from the account which the govt now insists came from Hassanshahi).

11. In the first affidavit date 2012, the agent makes no mention of any TECS inquiry. Therefore, presumptively, this information was not obtained or relied upon in ordering the LAX computer search.

In the affidavit filed in response to this motion to suppress, for the first time, the agent claims he consulted TECS in October 2011 and found a record of an "investigation" of Hassanshahi in 2003 -- some eight years before the ordered computer search. There were no charges brought and no interviews. This TECS "hit", even if considered, did not indicate any criminal activity in 2012, the year of the search. Nor did a border entry in 2006 which, again, did not result in Hassanshahi's being investigated or charged with any wrongdoing.

12. In short, even if all the data is considered including the database search, there was no indication any crime was "afoot" in 2012, at the time of the search. Contrary to the government's implication, merely crossing the border was not a crime.

ANALYSIS

I. THE GOVERNMENT'S FORENSIC EXAMINATION OF MR. HASSANSHAHI'S COMPUTER WAS NOT "FREE" BUT REQUIRED REASONABLE SUSPICION OF CURRENT AND ONGOING CRIMINAL ACTIVITY

A. Although the government wishes otherwise, Cotterman is the law in Los Angeles where the search initiated and will probably be expanded throughout the country.

The government challenges the Ninth Circuit's reasoning behind Cotterman but that is quite beside the point. Cotterman is the law in Los Angeles. The government required reasonable suspicion to conduct the forensic search of Mr. Hassanshahi's computer upon his entering at Los Angeles. That is the law of the Ninth Circuit where the border was crossed.

And Cotterman may soon be the law elsewhere as well. Recently the Supreme Court in California v. Riley recognized the unique and strong privacy interest of American's in their cell phones which, as the Supreme Court recognized, function like minicomputers. Indeed the "computer-like" data storage and processing capability of the mobile phones, makes them worth of Fourth Amendment protection. "Cell phones place vast quantities of personal information literally in the hands of individuals." 134 S. Ct. at 2485. The Supreme Court thus held that examining the digital contents of a mobile phone seized during an arrest, requires a search warrant This is the same justification for heightened protection for computer searches in Cotterman:

> Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's

> specific guarantee of the people's right to be secure in their "papers."

709 F.3d at 964.

In a similar case also involving a border-crossing forensic computer examination and alleged Iran sanctions violation, the federal district court in Maryland also concluded that reasonable suspicion is required. Saboonchi, 990 F. Supp. 2d 536 (D.Md. 2014). That court, like Cotterman, also rejected the government's argument that a forensic computer examination incident to a border crossing fell without the "border search" exception and required no reasonable suspicion or indeed any reason at all.

Saboonchi noted, in a long and reasoned opinion, that a forensic computer search differs in material ways from a simple "look-see" or even "turn on and look" of the computer at the border. 990 F. Supp. 2d at 547:

> A computer forensics expert will use specialized software to comb through the data, often over the course of days, weeks, or even months, *id.* at 537-38, searching the full contents of the imaged hard drive, examining the properties of individual files, and probing the drive's unallocated "slack space" to reveal deleted files.
> . . .
> Electronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel. A person's digital life ought not be hijacked simply by crossing a border. When packing traditional luggage, one is

> accustomed to deciding what papers to take and what to leave behind. When carrying a laptop, tablet or other device, however, removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files. It is also a time-consuming task that may not even effectively erase the files.
> . . . .
> . . . Such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity.
>
> [A] forensic examination of a computer or other electronic device using sophisticated technology-assisted search methodologies can exceed vastly the capacity of a human searching and viewing files. Moreover, this type of search exposes a class of data that raises novel privacy concerns, including files that a user had marked as "deleted"[9] and location data that may provide information about activities in the home and away from the border. For this reason, a forensic search of an electronic device differs significantly from a conventional search not merely in degree, but in kind. Accordingly, as explained below, **a forensic search of an electronic device seized at the border cannot be performed absent reasonable, articulable suspicion.**

B. "Reasonable suspicion" puts the burden on the government to articulate *facts* that a crime is currently afoot.

The reasonable suspicion standard puts the burden on the government to prove by a preponderance a "reasonably articulable suspicion for believing that criminal activity [is] afoot." Beck, 140 F.3d at 1134; Williams, 878 F. Supp. 2d at 197 ("The government bears the burden of proof, and under *Terry*, the government must present evidence that the police officer was able to articulate the specific facts that caused him to view

the defendant as a likely suspect."

C. The government fails its burden in this case because it refuses to disclose the central fact: the nature of the database that yielded Hassanshahi's telephone number.

The only current crime posited or being investigated here, was the possible sale of electrical equipment to Iran. Prior to the forensic examination of his computer, Mr. Hassanshahi's only "connection" to that crime, was the single alleged telephone call between a number on Sheikhi's email and the 818 number allegedly associated with Hassanshahi.

This is significant. All the other connections, real or imagined, (such as Hassanshahi's single telephone call to another number in Iran, or (possibly) accessing his google account from Iran, were innocent. Reasonable suspicion cannot be founded upon a "hunch or on circumstances that describe a very broad category of predominantly innocent travelers." Beck, 140 F.3d at 1136. Even the alleged 2003 TECS investigation, which did not result in any charges or even an interview, does not indicate any *current* criminal activity. (Otherwise, the government could freely stop and frisk every long-released and rehabilitated felon on the street solely because of the past conviction -- and Mr. Hassanshahi has no conviction.)

The sole claimed source of the Sheikhi telephone call to 818, is the undisclosed, undescribed and mysterious database. The government refuses to disclose any information about this database: what is it, is it reliable, *does it even exist?* For all that appears, the database is a cover for an inarticulable hunch, which will not support reasonable suspicion.

The initial burden is not on defendant to show the database is unconstitutional or unlawfully operated. Rather, the initial burden is on the government to demonstrate reasonable suspicion. Just like any party with the burden of proof, the government fails that burden when it refuses to disclose relevant facts, here, the nature, reliability, etc. of the database. Without that information, the government's claimed connection between Sheikhi and Hassanshahi, is simply an "inarticulable hunch." This is insufficient, and the search must be suppressed.

II. THE SUBJECT DATABASE IS EITHER THE NSA DATABASE OR ONE JUST LIKE IT AND SUBJECT TO THE SAME CONSTRAINTS

The subject database, as described, is identical in form, content and function as the NSA database. If it is not the NSA database, it is a copy of it.

The government actually presents no evidence that the database is not the NSA database. The government makes this claim in its memorandum, but there is nothing in the affidavit. Attorney argument in the memorandum is not evidence.'

The government cannot avoid the legal and potentially constitutional restrictions on the NSA database, by either using the same database in another department, making a copy and using that, or maintaining another database identical in all respects. The same rules must apply. The same rules were broken.

III. NO APPLICABLE THEORY PURGES THE VIOLATION AND RENDERS THE EVIDENCE USABLE

A. Evidence obtained through an otherwise lawful search which is derived from an illegal search, is excluded.

Evidence obtained through an otherwise lawful search, which was however conducted as a result of an unlawful search or

seizure, is itself inadmissible. For example in Beck, police stopped defendant's car and detained him. Once in detention, police conducted an otherwise lawful inventory of the car incident to detention and found incriminating evidence. The court held the police lacked reasonable suspicion to stop Beck's car in the first place. Because detention was unreasonable, evidence (otherwise lawfully) obtained incident to detention, was itself inadmissible. "The evidence of drug trafficking obtained during Beck's renewed detention was tainted by the unlawfulness of that detention and should have been suppressed." 140 F.3d at 1140.

Similarly, because the database inquiry led directly and proximately to the forensic computer search at LAX, the result of the computer search must also be suppressed. Wong Sun v. United States, 371 US 471, 484-86 (1963).

B. The controlling case is Scios which is directly on point.

The D.C. Circuit's *en banc* decision in Scios, 590 F.3d 956, is controlling and on point against the government in this case.

In Scios, a telephone lineman found extra wires connected to Your Pharmacy Service, a pharmacy in Washington DC. The investigation led to private investigator Scios. The FBI arrested Scios at his house but did not obtain a search warrant.

During the arrest, while Scios was fully restrained and subdued, an agent went through file folders in Scios' house and found a folder labeled Your Pharmacy Service. The file contained a Washington DC motel bill in the name of "Massa." Using the motel's record of telephone calls placed from the

room, the FBI found the potential witness Thomas Massa Jr. Id. at 958.

Massa was brought before the grand jury, immunized, and thereby compelled to testify against Scios. Scios was thereby convicted. Id. at 959.

Scios moved to suppress the Massa testimony as the fruit of an unlawful search of his house and the folder. The court easily concluded the search of the folder was not properly incident to arrest and was unconstitutional. The question was whether Massa's testimony could be used under the "attenuation," "independent source" or similar doctrines that "purged" the taint of the illegality. Id. at 960.

As is obvious, the case is similar to the instant case. Here as well, an initial improper search (use of the database) led to a telephone number. The telephone number led directly to evidence (Massa's testimony).

This Circuit followed Wong Sun, 371 U.S. at 478, which held the test is "whether the evidence to which instant objection is made has been come at by exploitation of the primary illegality or instead by means sufficiently distinguishable to be purged of the primary taint." In this regard, not every "but for" connection between illegal search and evidence means the latter evidence is out. On the other hand, some strong attenuation or an independent legal source must be shown to avoid suppression.

In Scios, the Court held the connection required Massa's testimony to be excluded. The court held (at 961):

> The claim, in substance, is that there was no direct link between the file folder and Massa, because the file document that showed

> Massa's name in the record of the motel room paid by defendant did not establish his identity. That only appeared when the police checked the motel's telephone records.
>
> We must begin with the illegal search. At the arrest for the offense of tapping the line of Your Pharmacy Service, the agent unlawfully riffled through defendant's file folders and removed his file for Your Pharmacy Service. **The agents tracked the Massa lead found in that file. They did not pursue a trail independent of the illegal search. The location of Massa was not the product of an improbable, unforeseeable coincidence. It was good police work, but a straightforward exploration of the leads in the Pharmacy file.** The fact that the exploration took some time, although a material consideration, does not of itself demonstrate that the exclusionary rule is inapplicable. **"The road . . . may be long, but it is straight."**

Similarly here, the agent tracked the database lead (allegedly connection Sheikhi's number to the 818 number linked to Hassanshahi). The agent did not pursue any trail independent of the 818 number disclosed by the database. This is important. The agent did not simply use the 818 number to identify Hassanshahi. The agent used the 818 number as the sole alleged connection (tenuous as it was) between Hassanshahi and Sheikhi and thus to possible wrongdoing. All other leads -- the google search, etc. -- proceeded directly from the 818 number disclosed by the database. There were no other leads and no other trails. As in Scios, the LAX search "was not the product of an improbable, unforeseen coincidence." Just like Massa's testimony in Scios, the computer search in this case is fruit of the poisonous tree and should be suppressed.

C. The govt's cases are mis-cited and inapposite.

Govt argues that in Friedland, the agents identified Friedland through an illegal wiretap but were nonetheless allowed to use the evidence against him. This is a misreading of the case. Friedland held (441 F.2d at 857) that the government was already investigating Friedland independently of the wiretap:

> In late 1963 or early 1964 Special Agent Best of the FBI was assigned to a squad investigating transactions in forged, counterfeit and stolen securities. He testified that he had never heard of any bugging involving Friedland until after the latter's conviction; that checking of the relevant FBI files showed that his squad had never received any memoranda containing information from the "bugs"; and that he never acquired information from any source concerning the activities of Friedland that were the subject of the bugged conversations -- or at least any that he used. His squad's interest in Friedland was triggered by cases where it was investigating another individual and "Mr. Friedland's name would come up either as being around a source of spurious securities or one that individuals had gone in or had gone into his office or something."

Friedland bears no relation to the instant case, in which the government's sole tie to Hassanshahi was through the telephony database.

In Najjar, in 1995 there was an improper search of Clinton Auto Sales, operated by Najjar. The search uncovered suspicious salvage title reports signed by Maryland State Police Officer Michael White. County Police officer Brown followed up on White, but the State Police impeded the investigation. Brown

regrouped and obtained all salvage titles signed by White from State records and other sources (including copies of the titles obtained from the search warrant). Brown therein saw many references to Najjar. This investigation took two years. Brown then sought and executed a new warrant on Clinton Auto Sales in 1997. 300 F.3d 466, 476.

Najjar challenged the results of the 1997 search warrants as alleged derived from the 1995 unlawful search. The court disagreed. "To determine whether the fruit is no longer poisonous, we consider several factors, including: 1) the amount of time between the illegal action and the acquisition of the evidence; 2) the presence of intervening circumstances; and 3) the purpose and flagrancy of the official misconduct." Id. at 477.

In Najjar, (1) two years of investigation passed between the 1995 unlawful search and the 1997 search that yielded evidence against Najjar. (2) the investigating officer obtained the information from independent sources such as State records. As the court held (at 479):

> In short, Wright'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 once Wright encountered the impediment at the Maryland State Police Barracks. The result of this investigation was that the *public* records seized from Clinton Auto Sales were rediscovered from independent sources. Because the documents subsequently came into Wright's possession independently, they cannot be the result of the primary illegality.
> . . .
> Even if the original illegal search in some

> slight way was a but-for cause of the later searches, Wright's two-year investigation and the intervening circumstances were sufficient to break the causal link between any primary illegality and later obtained evidence.

As to (3), the court found no intent to deceive or withhold information from the magistrate in the first search warrant. For all of these reasons, the court did not suppress the evidence.

The instant case is far different. As to factor (1), 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 US. There was no time for any independent investigation. As to (2), there was no independent source of information. The sole source connecting the 818 number and thus Hassanshahi to Sheikhi, was the telephone database.

As to (3), there is apparently misconduct and intent to deceive, or at least to conceal. The reality is that if the government had nothing to hide, it would disclose information about the database. No national security interest is claimed (indeed the govt pretends this is not the NSA database). The government cannot conceal all details of its activities and then claim good faith.

IV. THERE WAS NO REASONABLE SUSPICION FOR THE FORENSIC COMPUTER SEARCH EVEN WITH THE DATABASE

Even considering the database, prior to the computer search, the government had no suspicion of and no information even suggesting Hassanshahi was involved in a *current* crime of any kind. The closest was the single possible telephone contact

between Sheikhi and the 818 number suggested by the database. Without content, or at least a pattern of calls, this cannot suggest criminal activity. As defendant's cases cited in the motion demonstrate, even clear contact between the defendant and a known drug dealer does not give reasonable suspicion to stop the defendant. Under govt's theory, the registered owner of every telephone number found to have called or been called by the number of a known drug dealer, can be stopped and frisked for drugs. That is not the law.

That Hassanshahi may have been investigated in 2003, or was briefly detained (the record indicates a 5 hour detention and gives no purpose for the detention) while crossing the border in 2006, does not indicate a possible ongoing crime in 2012. Under this theory, every person once convicted of a drug felony -- let alone once investigated for drug dealing -- could be stopped and frisked on sight, forever, including long after release from prison and rehabilitation. That is not the law for once-convicted drug dealers, let alone for Hassanshahi who has no criminal record of any kind.

Even a prior criminal record is not, standing alone, sufficient to create reasonable suspicion. United States v. Davis, 94 F.3d 1465, 1469 (10th Cir. 1996). There must be other "concrete factors" to demonstrate that there was a reasonable suspicion of *current* criminal activity. United States v. Sandoval, 29 F.3d 537, 542 (10th Cir. 1994). And "just as an officer's knowledge of a suspect's past arrests or convictions is inadequate to furnish reasonable suspicion; so too is knowledge that a suspect is merely under investigation, which is

an even more tentative, potentially innocuous step towards determining criminal activity." United States v. Foster, 634 F.3d 243, 248 (4th Cir. 2011). How much less probative is the agent's (current revised) claim that Hassanshahi was investigated *and cleared* back in 2003. If anything, prior investigation without charges indicates a lack of criminal activity.

By contrast in US v. Ali Saboonchi, the government found substantial direct documentary evidence tying Saboonchi to current criminal conduct. Indeed the Saboonchi record illustrates the clear difference between reasonable suspicion for the subsequent computer search, found in Saboonchi, and the lack of reasonable suspicion in this case. In Saboonchi, 990 F. Supp. 2d at 542, the investigation began in 2010:

> [FBI Special Agent Kelly] Baird testified that Saboonchi first came to the attention of federal authorities in the Fall of 2010, when "the FBI received information that there had been an inquiry to a company in Vermont regarding specialized technology that has applications with industrial medical or military applications" by "a person named Ali," whose telephone number eventually led to Saboonchi.

This first investigative step has a surface similarity to the instant case, in that a company inquiry led to a telephone number that led to the defendant. But in Saboonchi, the government knew the phone call was actually to purchase sensitive military goods. Here, the govt has no idea the substance, duration or even the parties to the alleged call between Sheikhi and the 818 number linked to Hassanshahi.

Nor did the government stop with a phone number in

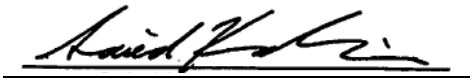
Saboonchi. Instead, the government subpoenaed and obtained shipping records that showed Saboonchi had, in fact, shipped a "cyclone separator" to a company in United Arab Emirates, which company was linked to Iran. Id. at 542. Baird then interviewed personnel at a manufacturer who said Saboonchi had purchased cyclone pumps to them but represented the end user was domestic. This contradicted the shipping records to UAE. Only after this and further investigation indicated current criminal activity by Saboonchi, did the government order a forensic search of Saboonchi's computer when he next crossed the border.

The pre-search investigation in Saboonchi indicated current criminal activity. By contrast, none of the information obtained in this case before the LAX search, indicated Hassanshahi was involved in a current crime of any kind. At most the agent had a hunch. More likely, the agent knew Hassanshahi was overseas and would travel back, so he took advantage to order a full forensic search. He probably believed -- as the government still claims -- he needed no reasonable suspicion or any other basis for the search. It was purely speculative and opportunistic.

And herein lies the greatest problem and need to suppress the evidence. Cotterman, Riley and Saboonchi all understand the public has a heightened Fourth Amendment interest in their personal data devices, whether mobile phones or computers. A forensic computer examination of the type conducted here, is an extreme intrusion upon a recognized privacy interest. If reasonable suspicion is not required, the government can conduct such a search any time it pleases incident to a border crossing.

The government can even "flag" individuals -- any individuals it chooses, with or without reason -- for such search "when and if" they cross a border. This was done in the instant case. Only by requiring and then enforcing the need for reasonable suspicion, can the courts restrain this governmental intrusion on personal privacy.

DATED: November 3, 2014



Saied Kashani
California State Bar 144805
800 W. 1st St. Suite 400
Los Angeles, CA 90012
tel. (213) 625 4320

Attorneys for Defendant
SHANTIA HASSANSHAHI

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing opposition was served electronically on Frederick Yvette, counsel for the government, via email to Mr. Yvette's confirmed email address on November 3, 2014.

/s/ Saied Kashani
Saied Kashani