JOHN P. PIERCE
DC Bar No. 475101
Themis PLLC
2305 Calvert Street NW
Washington, DC 20008
tel. (202) 567-2040
fax (202) 567-2051
email: JPierce@Themis.US.com

Attorneys for Defendant
SHANTIA HASSANSHAHI

UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. SHANTIA HASSANSHAHI, Defendant.	Case No. 13-CR-274-RC-1 Mag. No. 13-014 **DEFENDANT'S MOTION TO SUPPRESS EVIDENCE [FR Crim.P 12(b)(3)(C)]** **[ORAL ARGUMENT REQUESTED]** **Next hearing date:** **April 24, 2014**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTRODUCTION AND SUMMARY

Defendant Shantia Hassanshahi, a U.S. citizen with no criminal record, is accused of some involvement in importing or attempting to import certain civilian electrical equipment to a private company in Iran. It is not clear from the complaint whether the equipment actually made it to Iran. It is undisputed that the equipment in question is non-military, non-nuclear-related and non-high-tech. **There is no accusation or suggestion whatsoever of violence or terrorism.**

All of the evidence against Mr. Hassanshahi came from or was directly derived from an offsite, multi-week, intensive forensic search and copying of all data and every file on the laptop computer and accompanying memory storage devices (thumb drives etc.) that accompanied Mr. Hassanshahi on his return to the United States through customs at Los Angeles International Airport on January 12, 2012. There was no search warrant.

According to the government's affidavit (attached as Exhibit A), the government conducted the forensic computer search of the computer as the direct and proximate result of information obtained from a massive historic database of telephone call log records. This is undoubtedly the so-called Bulk Telephony Metadata Program or some variant thereof, which has been in the news of late. The government claims it found records in the said database of an unspecified number of telephone calls, of unspecified duration, between an 818-area code number associated in some manner with Mr. Hassanshahi and a number in Iran associated with a person who may have been

seeking to purchase the electrical equipment.

The government does not have and does not claim to have recordings of the actual calls. Thus the government lacked, and still lacks, any evidence that the import of any goods, or indeed any suspicious topic of any kind, was actually discussed in the subject telephone calls. For all the government agents knew then or know now, the calls were purely personal or family-related. Indeed the agents did not and do not even know if Hassanshahi - or for that matter the person of interest in Iran – was actually on any of the calls. The database indicates only that a call was placed from telephone number X to telephone number Y, *not* who was actually on the call or what if anything was said on the call. Moreover, the 818 number is a Google internet number, so the call could literally have been placed from a computer terminal anywhere in the world by anyone with access to the Google account.

In any event it is undisputed that *but for* the use of the Bulk Telephony Metadata Program (BTMP) or an equivalent database, the government would not have had any interest in Mr. Hassanshahi and would not have conducted the computer search at all. There was no informant, no email and no other basis to focus on Mr. Hassanshahi *except* that which was obtained from using the BTMP database.

Defendant Hassanshahi accordingly moves to suppress all evidence obtained from the forensic examination/copying of the computer and related memory devices on the following grounds:

1. This Court, in Klayman v. Obama, 957 F. Supp. 2d 1, 41

(D.D.C. Dec. 16, 2013)(J. Leon), recently determined, in the context of an order issued pursuant to a request for preliminary injunction, a "substantial likelihood" that the BTMP is an unreasonable search under the Fourth Amendment. If maintenance or use of the BTMP (especially without a specific warrant) is an unreasonable search, then any information directly derived from said use is "fruit of the poisonous tree" and should be suppressed. All data, documents and information obtained from the forensic search of the computer in this case should therefore be suppressed. United States v. Six hundred Thirty-nine Thousand Dollars, 955 F.2d 712, 719 (D.C.Cir. 1992) ("evidence obtained by exploiting the Fourth Amendment violation" shall be excluded.)

2. Even assuming the BTMP is constitutional, the governing orders and statutory authority provide that the BTMP database may only be consulted, without judicial approval, through use of "identifiers" (such as names or telephone numbers) associated with ***terrorist activity***. Klayman, 957 F. Supp. 2d at 16. There was never any suggestion of terrorist activity in this case. Thus, use of the BTMP or an equivalent database, as was apparently used here, was outside even the government's own internal orders and authority.

To summarize (1) and (2), either the database is unconstitutional, or the government did not follow its own rules and limitations restricting use of the database to terrorism issues. Either way, use of the database in this case was unconstitutional or unlawful and evidence derived therefrom

should be suppressed.

3. If the subject database was not the BTMP or an equivalent program, then defendant requests discovery and an evidentiary hearing to determine the nature, governing authority and prescribed limitations for the database utilized in this case. Defendant notes that whatever the specific database was, it *necessarily* resembles the BTMP in all constitutional respects: it is comprehensive, historic and aggregates data regarding telephone calls placed to or from U.S. citizens who are not under any suspicion of wrongdoing.

4. There are additional grounds for suppressing the evidence. When a computer search is conducted at Los Angeles International Airport ("LAX"), "reasonable suspicion" is required to conduct and sustain a comprehensive forensic computer/memory examination of the type conducted in this case. United States v. Cotterman, 709 F.3d 952, 963 (9th Cir. 2013). This is the type of articulable suspicion that would support a "Terry" stop and frisk in the street. The government's affidavit does not support reasonable suspicion for the computer examination in this case. If it did, by analogy, the government could "stop and frisk" everyone entering or leaving a house associated with a mobile phone number from which calls had been placed, at some point, to a suspected drug dealer, without any proof that any of the individuals had even actually spoken with the dealer much less had an illegal interaction with him. That is not the law. See, e.g., Washington v. Gilmore, 1998 U.S.Dist. LEXIS 17309, 1998 WL 774629 (N.D.Cal. Oct. 30, 1998)

(suspect's "huddling" with a known drug dealer did not constitute "reasonable suspicion" to stop and frisk suspect absent some additional basis to infer criminal activity).

STATEMENT OF THE CASE

This factual statement consists of (a) facts taken directly from the government's affidavit of Special Agent Joshua J. Akronowitz, attached to the complaint; (b) general background information or facts clearly appearing from the affidavit; and (c) facts inferable from the government's affidavit. **If any facts are disputed by the government, Mr. Hassanshahi requests an evidentiary hearing to determine any disputed facts.** The following typefaces are used for reference:

This typeface is used for text copied directly from the government's affidavit.

Additional general background facts that should be undisputed (such as the nature of Google phone accounts) are presented in this plain typeface.

Facts that are inferable from the government's affidavit are presented in this italic typeface.

FACTUAL STATEMENT

Fact No. 1:

On August 16, 2011, an HSI-DC agent received an unsolicited e-mail from a voluntary source associated with this investigation (the "Source" or "IT"), indicating that the Source had received a request from "M. Sheikhi" ("Sheikhi"), on behalf of "Radyab Bartar Company," to buy protection relays manufactured by a company identified herein as "COMPANY A." The Source stated that IT had information that "Sheikhi" sought the protection relays for use in an Iranian power project, but IT would only discuss the matter further with HSI agents in person.

Fact No. 2:

Protection relays are used for civilian electrical supply. They are not military, nuclear or high-technology items. **There is no suggestion of terrorism or violence in this case.**

Fact No. 3:

Based on the above information, on or around September 20, 2011, I and another HSI-DC agent interviewed the Source. During the interview, the Source summarized his prior contacts and conversations with "Sheikhi", stating, in sum and substance:

Fact No. 4:

a. On or around August 6, 2011, "Sheikhi" e-mailed the Source and solicited the Source's assistance in procuring U.S.-origin protection relays for "Sheikhi's" company, Radyab Bartar Company, located in Iran. "Sheikhi" advised the Source that "Sheikhi" traveled to Vienna often, had an office there, and proposed that "Sheikhi" and the Source do business there.

Fact No. 5:

b. "Sheikhi" also asked the Source whether, based on the Source's past professional experience, the Source would serve as a broker for the procurement of U.S.-origin protection relays for use in Iran. In particular, "Sheikhi" asked the Source to identify U.S.-based entities with ties to "COMPANY A" that could assist with procuring protection relays from COMPANY A for export and end-destination in Iran. "Sheikhi" further told the Source that if the Source was successful in brokering the procurement of protection relays from COMPANY A in this instance, "Sheikhi" may seek to include the Source in similar and more profitable procurement transactions in the future. The Source also gave HSI a copy of the above-referenced e-mail sent by "Sheikhi" to the Source.

Fact No. 6:

A subsequent government affidavit identified COMPANY A as Areva, a French company.

Fact No. 7:

There was and is no suggestion whatsoever of terrorism or violence of any kind.

Fact No. 8:

There is no evidence or suggestion "Sheikhi" was or is involved or connected in any way with terrorism or violence.

Fact No. 9:

The "Source" did not identify or refer in any way to defendant Shantia Hassanshahi. There was and is no evidence that Sheikhi's email that referred to procuring relays, was sent to defendant Hassanshahi. No informant, anonymous or otherwise, ever referred to Mr. Hassanshahi.

Fact No. 10:

After interviewing the Source, I independently sought to corroborate the Source's information concerning "Sheikhi" and "Radyab Bartar Company," and their purported interest in procuring U.S.-origin protection relays manufactured by "COMPANY A" for use in Iranian power grids. My investigation revealed the following:

Fact No. 11:

a. A review of "Sheikhi's" business card, which was included in the e-mail from "Sheikhi" to the Source, indicated that: (1) "Sheikhi's" full name is Manouchehr "Sheikhi"; (2) "Sheikhi" purports to be the "General Manager" for Radyab Bartar Company; (3) the business address listed for Radyab Bartar Company is in Tehran, Iran; (4) the listed business telephone numbers for "Sheikhi" at Radyab Bartar Company begin with "98"—the country code for the Islamic Republic of Iran.

Fact No. 12:

The affidavit does not reveal the actual telephone number on Sheikhi's business card.

Fact No. 13:

b. According to open source information, Radyab Bartar Company's website, www.radyabco.com, was registered with Night and Day Designers at www.shaborooz.ir, and by a registrant having an address in Tehran, Iran. Based on my experience, I know that website domain addresses having the suffix ending in "ir" resolve to Iran.

Fact No. 14:

There is no claim that Sheikhi's name, email, company name, telephone number was associated with terrorist activity (for example, that a call had ever been placed from a telephone number of a known terrorist to Sheikhi's number).

Fact No. 15:

c. According to open source information, COMPANY A is an international company based in France with manufacturing plants and offices in the United States, Canada, and Australia, specializing in the business of manufacturing sophisticated protection relays for use in various electrical systems, including electrical power grids.

Fact No. 16:

Using the business telephone number associated with "Sheikhi", I searched HSI-accessible law enforcement databases, in furtherance of identifying potential U.S.-based targets engaged in the sale or export of protection relays for use in the Iranian electrical power grid. As a result of my search, I discovered telephone call log records indicating that a number of telephone calls between "Sheikhi's" known business telephone number and telephone number 818-971-9512 had occurred within a relatively narrow time frame. Based on my training and experience, I know that area code "818" is an area code originating in Los Angeles County, CA.

Fact No. 17:
There was no use of a "pen register" or other surveillance, authorized or otherwise, of Sheikhi's telephone number or email address, at any time.

Fact No. 18:
The "HSI-accessible law enforcement databases" appears to refer to the Bulk Telephony Metadata Program or some equivalent bulk telephone data collection program. This is a program under which the United States Government has been collecting and retaining a record of essentially every telephone call to or from every United States telephone number. At a known minimum, the government has collected and retained information including: the number from which the call was placed, the number dialed, and the date/time and possibly the duration of the call. Klayman v. Obama, 957 F. Supp. 2d 1, 14 (2013). Importantly, the program and the database collects and retains phone call data from and involving more or less all Americans, without prior evidence of, indeed without regard to, wrongdoing or even alleged wrongdoing. Simply put, details of every call placed or received by anyone, go into the database.

Fact No. 19:
Alternatively the government utilized some other historic, comprehensive database of calls placed to and from U.S. phone numbers of U.S. citizens not suspected of any wrongdoing at the time of data collection. For example this might be a database of phone records of every call ever placed to or from Iran to or from any telephone number in the United States. If the database were operated in some other fashion, it would not have contained the data retrieved or would not have been searchable in the manner. Therefore in every constitutional respect, the utilized database resembles the BTMP subject of Klayman.

Fact No. 20:
It appears the government "queried" the database by inputting

Sheikhi's telephone number (the "query") on Sheikhi's card (on the email to Source) and retrieved all calls placed to/from any U.S. telephone number to the Sheikhi number.

Fact No. 21:
There was no search warrant or other judicial authorization for the search.

Fact No. 22:
The search was not conducted through a "query" using an "identifier" (e.g. name, telephone number, etc.) associated with terrorist activity.

Fact No. 23:
There is no evidence given of the date, specific frequency or duration of the calls from the "Sheikhi" phone number to 818-971-9512.

Fact No. 24:
The government had, and has no evidence as to who *was on the calls, at either end (Sheikhi's phone number or the 818 number).*

Fact No. 25:
The government had, and has no evidence of what, if anything was discussed on any of the telephone calls. In particular, there was, and is no evidence that any wrongdoing of any kind was discussed on the calls. All that appeared at the time and still appears, these were personal calls with no business component.

Fact No. 26:
Telephone number 818-971-9512 was and is a Google phone number (see below from Exhibit A).

Fact No. 27:
Google phone numbers are not landlines and are not confined to any geographic location. The user is given a choice of area codes when setting up the account, and can select any area code anywhere in the U.S.

Fact No. 28:
Any person with the username and password, not just the person who set up the account, can access the Google phone number and place and receive calls from/at the Google phone number from any Internet connection in the world.

Fact No. 29:

On or about October 6, 2011, I prepared and served an Administrative Export Enforcement Subpoena for subscriber information for telephone number 818-971-9512 on Google, Inc. ("Google"), the U.S.-based service provider. In response, Google produced the following subscriber information for the telephone number:

Name:	Shantia **HASSANSHAHI**
E-mail:	shantia34@gmail.com
Address:	1636 Castlehill Ct., Westlake Village, CA 91361
Alt Phone Number:	805-857-4669
Created on:	2010 Jun 17 09:52:20
Signup IP:	72.134.19.172

Fact No. 30:
This information reveals and revealed only that the above name and address was input when the Google telephone number account was set up.

Fact No. 31:
The government did not check any billing information to see if Shantia Hassanshahi was actually paying for the Google telephone number.

Fact No. 32:
In any event, as explained above, given the nature of the telephony database and the Google phone number, the government had no evidence that defendant Hassanshahi was actually on any of the alleged phone calls, or that anything substantive or unlawful was discussed by anyone on the calls.

Fact No. 33:

In addition, Google produced call log information for the telephone number during the period of September 6, 2011, to October 6, 2011, which revealed numerous outgoing calls made to telephone number 98-938-1911602. Again, based on my training and experience, I know that the country code for the Islamic Republic of Iran is "98." Accordingly, it appeared that **HASSANSHAHI**, using a U.S.-based telephone number suspected of having a connection to the suspected procurement network (i.e., 818-971-9512), made numerous calls to the same Iranian-based telephone number during a relatively finite period of time.

Fact No. 34:
The government's affidavit **does not contend** that the Iranian telephone number given, 98-938-1911602, is that of Sheikhi. Indeed the affidavit does not reveal Sheikhi's telephone number. Therefore, while the affidavit is carefully worded to imply, without so saying, that 98-938-1911602 is Sheikhi's number, in

fact this is never stated or claimed and it is therefore **not** Sheikhi's number.

Fact No. 35:
*The only inference is that 98-938-1911602 is **not** Sheikhi's number. Therefore, all the government knew or now knows is that in September-October 2011, calls were made from 818-971-9512 to 98-938-01911602, a number associated with Iran but **not**, so far as appears, Sheikhi.*

Fact No. 36:
The affidavit is also carefully worded to imply, without so saying, that the September-October 2011 phone calls are the same as the calls retrieved from the telephony database between 818-971-9512 and Sheikhi's business number. This in turn implies that the calls between the 818 number and Sheikhi's business number took place in September-October 2011. But in fact this is never actually stated and this is not the case. The September-October 2011 telephone calls referenced in the affidavit, were to a different number unrelated to Sheikhi.

Fact No. 37:
Again, because 818-971-9512 is a Google number, the September-October 2011 calls, or any calls anytime from 818-971-9512 could have been placed by anyone, at any location in the world, and not necessarily by Mr. Hassanshahi.

Fact No. 38:
Even assuming Mr. Hassanshahi placed the September-October 2011 calls, these calls were entirely personal or to a family member and bore no relationship to Sheikhi or to business of any kind.

Fact No. 39:

Based on the above information, on or about December 20, 2011, I prepared and served an Administrative Export Enforcement Subpoena for subscriber information and recent Internet protocol logs for HASSANSHAHI's purported e-mail account, shantia34@gmail.com, on Google. On January 10, 2012, Google produced Internet protocol information concerning the e-mail account, which indicated that HASSANSHAHI accessed the e-mail account twenty-four times from December 8-15, 2011, while located in Iran.

Fact No. 40:
A Google email (or googlemail or "gmail") account can be accessed by anyone with the email address and password.

Fact No. 41:
Google keeps records of the IP address (or apparent IP address)

of the computer that accesses the googlemail account. It is this record that was produced to the government pursuant to subpoena. These records do not show, and cannot show, which *individual* accessed the account. Again, any person with the password can access the account.

Fact No. 42:
Contrary to the affidavit, the records obtained showed only that the gmail account was accessed from an IP address apparently in Iran, not that Mr. Hassanshahi was the person accessing the account.

Fact No. 43:
It is well-known in Internet circles, and should certainly be well known to the government affiant, that many people around the world utilize VPNs. A VPN is an internet service that disguises the user's true IP address. For example a user in Turkey might appear to have an IP address in Iran.

Fact No. 44:
The government never excluded the possibility of use of a VPN in connection with the subject Google telephone number or email account.

Fact No. 45:
Because a VPN could have been used, the government could not have and cannot be sure of the true location, let alone identity, of the person who accessed the subject email account.

Fact No. 46:
Contrary to the affidavit, because of the nature of the Google account and the possible use of VPNs, the government had no conclusive information that defendant Hassanshahi accessed the email account, or that the account was accessed from Iran.

Fact No. 46:
There was no evidence of any emails from the subject Google email account to or from Sheikhi's email account.

Fact No. 47:

On January 11, 2012, I received information indicating that HASSANSHAHI would be flying into the Los Angeles International Airport (LAX) on Lufthansa Airlines (LH) flight #456 from Frankfurt, Germany. Accordingly, I requested that HSI Los Angeles, CA (HSI-LAX) conduct a secondary examination of HASSANSHAHI upon his anticipated arrival into the United States.

Fact No. 48:

There was no search warrant or other judicial authorization for the forensic examination.

Fact No. 49:

On January 12, 2012, at approximately 12:40 P.M. PST, HASSANSHAHI arrived at LAX on flight #456 from Frankfurt, Germany. HASSANSHAHI presented himself for primary inspection to U.S. Customs and Border Protection (CBP) Officers in the Federal Inspection Service (FIS) area, who thereafter referred HASSANSHAHI to the secondary inspection area for further examination. At the time, HASSANSHAHI had in his possession a laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone (collectively, the "electronic devices"). CBP detained these items and turned them over to HSI-LAX, who subsequently mailed them to HSI-DC for electronic imaging.

Fact No. 50:

Hundreds of thousands of persons of Iranian descent live in Southern California.[1] Most are first-generation arrivals who still have family in Iran. Travel to Iran is long and expensive, thus, many Iranians stay a relatively long time in Iran on each trip. On any given day, hundreds if not over one thousand Iranians travel through LAX to or from Iran.

Fact No. 51:

Upon receipt, HSI-DC forensically imaged the electronic devices. Among other things, a review of the contents of the electronic devices, particularly the laptop computer, revealed the following:

. . .

[1] There are so many Iranian-Americans in Los Angeles that they even have their own reality television show on a major cable channel.

- **The below letter (translated from Farsi to English), dated September 5, 2011, authored by HASSANSHAHI and addressed to Majid Namjoo, the Iranian Minister of Energy, which detailed the Iranian Ministry of Energy's 2009 procurement of COMPANY A protection relays from HASSANSHAHI, through HASSTON, for use by the Fars Regional Electric Company in Iran. (The name of the company has been substituted with "COMPANY A" in the body of the letter below.)**

[and other evidence now utilized in the case]

Fact No. 52:
This was a comprehensive, detailed, forensic examination and copying of the entire computer and its contents, and the contents of all memory devices. This is not, by any means, a simple "turn on and look" at the computer.

Fact No. 53:
The computer examination took several weeks.

Fact No. 54:
The search was conducted in Washington DC, far from the airport where Mr. Hassanshahi crossed the border/entered the United States.

Fact No. 55:
The government would not have conducted the forensic examination of the computer but for the information obtained from the telephony database referenced in the government affidavit.

Fact No. 56:
Indeed, the government would not have focused any attention on Mr. Hassanshahi at all, but for information from the telephony database.

ANALYSIS

I. THE FILES AND RECORDS OBTAINED FROM THE COMPUTER SEARCH SHOULD BE SUPPRESSED AS FRUITS OF THE UNCONSTITUTIONAL BULK TELEPHONY METADATA PROGRAM

A. The case against Mr. Hassanshahi derives entirely from use of the Bulk Telephony Metadata Program or an equivalent program.

All of the evidence now utilized against Mr. Hassanshahi came directly from the computer search or was derived from the computer search. The government only conducted the computer search, and indeed only became interested at all in Mr. Hassanshahi in the first place, because of the BTMP.

No informant (anonymous or otherwise) suggested the government look at Mr. Hassanshahi. Mr. Hassanshahi's name never came up in discussions with the "Source" in Vienna, or anywhere on Sheikhi's email. The government did not subpoena or attempt to subpoena Sheikhi's email records, for example from an international email provider assuming Sheikhi utilized one.

The government also did not place an electronic "trap" or "pen register" on Sheikhi's phone or email account after learning of Sheikhi from the Source. Such a trap or pen register, assuming it was technically feasible, would have captured telephone numbers and email addresses contacted from Sheikhi's telephone number or email *going forward*, after the point that Sheikhi had come under suspicion. The installation, without a warrant, of a pen register or "electronic trap" to capture such data *going forward* from a specified telephone number *which has come under suspicion*, was approved in Smith v.

Maryland, 442 U.S. 735 (1979).

Instead, the government consulted an all-pervasive, all-encompassing *historic* database of previously dialed telephone calls. The agent put in Sheikhi's business telephone number and searched the database for all telephone numbers that had previously telephoned Sheikhi's number.

While the government's affidavit does not identify the database by name, this can only be the BTMP database or some equivalent. No other database could have supplied the necessary information.

B. What is the Bulk Telephony Metadata Program?

Defendant refers here to the detailed analysis undertaken in the opinion of this Court in Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. Dec. 16, 2013). The analysis is thorough and clear. Summarizing and quoting Klayman at 11,14:

> In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 *et seq.* ("FISA"), "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes.". . . Congress passed FISA "in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused. . . In enacting FISA, Congress also created two new Article III courts—the Foreign Intelligence Surveillance Court ("FISC"), composed of eleven U.S. district judges, "which shall have jurisdiction to hear applications for and grant orders approving" such surveillance, § 1803(a)(1), and the FISC Court of Review, composed of three U.S. district or court of appeals judges, "which shall have jurisdiction to review the denial

> of any application made under [FISA]," § 1803(b)
>
> In addition to authorizing wiretaps, §§ 1801-1812, FISA was subsequently amended to add provisions enabling the Government to obtain ex parte orders authorizing physical searches, §§ 1821-1829, as well as pen registers and trap-and-trace devices, §§ 1841-1846
>
> In broad overview, the Government has developed a "counterterrorism program" under Section 1861 in which it collects, compiles, retains, and analyzes certain telephone records, which it characterizes as "business records" created by certain telecommunications companies (the "Bulk Telephony Metadata Program"). The records collected under this program consist of "metadata," such as information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted.
>
> . . . According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those calls, or the names, addresses, or financial information of any party to the calls.
> . . .
> The Government has conducted the Bulk Telephony Metadata Program for more than seven years. Beginning in May 2006 and continuing through the present,[18] the FBI has obtained production orders from the FISC under Section 1861 directing certain telecommunications companies to produce, on an ongoing daily basis, these telephony metadata records, which the companies create and maintain as part of their business of providing telecommunications services to customers. The NSA then consolidates the metadata records provided by different telecommunications companies into one database, and under the FISC's orders, the NSA may retain the records for up to five

> years. According to Government officials, this aggregation of records into a single database creates "an historical repository that **permits retrospective analysis,**" enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers.
>
> In plain English, this means that if a search starts with telephone number (123) 456-7890 as the "seed," the first hop will include all the phone numbers that (123) 456-7890 has called or received calls from in the last five years (say, 100 numbers). . .
>
> [citations to government's affidavits provided in Klayman case omitted].

The government's affidavit in this case demonstrates that it utilized either the BTMP database described above, or some other database collected and utilized in the same fashion. In this case, the government used Sheikhi's business telephone number from his card on the email to Source as the "query" or "seed" (or (123) 456-7890 in the example above from Klayman). The query returned all telephone numbers that had placed or received calls to/from Sheikhi's number. This result included the 818 Google phone number claimed to be associated with Hassanshahi.

Essential characteristics of the BTMP, and, necessarily, of the database utilized in this case, include the following:

1. The data is collected and stored over several years.

2. The data collection is fully comprehensive. In the case of the BTMP, it essentially consists of every phone number

dialed to/from any U.S. number (or beyond), for years.

3. The data is collected without regard to, or claim of, any wrongdoing on the part of the persons whose data is collected. *Every* U.S. citizen's phone data is collected and put into the database indiscriminately. No court reviews and authorizes an advance determination that a particular person's data shall be collected (as in the manner of a pen register).

4. The data collection started some time ago, i.e., it is historic data. In this case, the agent ran the query after August 2011 but found prior calls. Therefore, necessarily, at the time the data was collected, there was no claim or suspicion of wrongdoing on the part of the persons whose data was being collected. **Data was being collected for possible, unspecified *future* use.** In a sense, the program collects data against every American today because one out of millions might, in the future, come under suspicion.

5. Data from telephones of U.S. citizens is collected and becomes part of the database. This is necessarily so, because the database used in this case retrieved an 818 telephone number the government claims is associated with a U.S. citizen, Mr. Hassanshahi. For this data to be in the database, the government must have been collecting the data from U.S. citizens *well before* the query.

C. The BTMP and the instant database are not pen registers.

A "pen register" or electronic "trap" is a physical or software device placed on or in respect of a specific telephone number or line. After placement, the device records all telephone numbers dialed from or dialing to the subject line.

Importantly, a pen register or equivalent device only operates prospectively and only on the specific phone line entrapped. Also, such a device requires some legal showing, for example FISA enables the government to obtain the trap with an ex parte application. 50 U.S.C. §§ 1841-1846. In practice this means the government can collect the data only after some showing of wrongdoing or suspected wrongdoing. Also, a pen register is a limited device utilized on a case-by-case basis.

Klayman noted the key *constitutional* differences between a pen register and the BTMP (957 F. Supp. 2d at 30-31):

> [In *Smith v. United States*, 442 U.S. 735 (1979)], [t]he Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed from his phone because he voluntarily transmitted them to his phone company, and because it is generally known that phone companies keep such information in their business records. The main thrust of the Government's argument here is that under *Smith*, no one has an expectation of privacy, let alone a reasonable one, in the telephony metadata that telecom companies hold as business records; therefore, the Bulk Telephony Metadata Program is not a search.

> The question before me is *not* the same question that the Supreme Court confronted in *Smith.* To say the least, "whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment," *id.* at 736—under the circumstances addressed and contemplated in that case—is a far cry from the issue in this case.
>
> For the many reasons discussed below, I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary, for the following reasons, I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.
>
> First, the pen register in *Smith* was operational for only a matter of days between March 6, 1976 and March 19, 1976, and there is no indication from the Court's opinion that it expected the Government to retain those limited phone records once the case was over.. . .This short-term, forward-looking (as opposed to historical), and highly-limited data collection is what the Supreme Court was assessing in *Smith.* The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years'* worth of data.
>
> . . . In *Smith*, the Court considered a one-time, targeted request for data regarding an individual suspect in a criminal investigation, *see Smith*, 442 U.S. at 737, which in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA now receives as part of its Bulk Telephony Metadata Program. It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect

> all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.
> . . .
> Third, the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979.
> . . .
> Finally, *and most importantly*, not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well.

Judge Leon accordingly held (at 32):

> I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

Accordingly, if we credit the government's analysis that the (818) number belongs to Mr. Hassanshahi, then (a) Mr. Hassanshahi had a reasonable expectation of privacy in his (818) telephone number data/metadata and (b) the government's bulk collection of said data constituted a search for purposes of Fourth Amendment analysis.

D. Use of the BTMP database or the equivalent database utilized in this case, constituted an unconstitutional search.

There is no doubt that the data in the BTMP and in the database utilized in this case was collected *and queried* without any warrant as to Mr. Hassanshahi or anyone else. Thus the collection and retrieval constituted a warrantless search. See

also Klayman, 957 F. Supp. 2d at 38.

Judge Leon further held that the warrantless search was not justified by any extenuating or other factors. Judge Leon noted that even historic telephony data as to a single suspect telephone number could be collected by search warrant on the telephone service provider on a case by case basis. Id. at 39. The government claimed, in response, that querying the database was *faster* and permitted *rapid* collection of the data in order to identify possible terrorist threats (at 40):

> Indeed, the affidavits in support of the Government's brief repeatedly emphasize this interest in speed. For example, according to SID Director Shea, the primary advantage of the bulk metadata collection is that "it enables the Government to *quickly* analyze past connections and chains of communication," and "increases the NSA's ability to *rapidly* detect persons affiliated with the identified foreign terrorist organizations."

Judge Leon held that the facts showed otherwise (at 40):

> Yet, turning to the efficacy prong, the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency.

(Importantly, speed of response to a terrorist threat is

not a consideration in this case, therefore even this justification is not present in the instant case. Indeed, in the instant case the government could have obtained search warrants or issued valid subpoenas for US telephony contacts with the Sheikhi number. No imminent threat of any kind justified use of the database instead of normal legal channels.)

Judge Leon accordingly held (at 41):

> Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment.

Plaintiffs in Klayman were telephone service subscribers who had reason to believe their telephone calling history and records had been swept up and stored in the BTMP database. These plaintiffs had most likely suffered a Fourth Amendment violation. Importantly, the violation was the mere collection and storage of the data, let alone retrieval of the plaintiffs' data as occurred in this case.

In this case as well, taking the government's affidavit as correct, the phone usage histories of Mr. Hassanshahi, a U.S. citizen, together with the histories of millions of other U.S. citizens, were swept up, aggregated and stored in the database utilized in this case. That database was either the BTMP itself or an equivalent program. Judge Leon's opinion in Klayman directs that use of that database constitutes an unreasonable search in violation of the Fourth Amendment.

E. The unreasonable search led directly and proximately to the computer search, therefore, all data obtained from the computer should be excluded.

The government's affidavit shows that the sole reason the government focused on Mr. Hassanshahi, and conducted the computer search at LAX, was because his number came up in the telephony database. There was no other reason to focus on or search Mr. Hassanshahi. The computer search in Los Angeles was specified in advance; it was not random. Thus, all the files, data and materials derived from the search, and subsequent information obtained as a result of seizing the computer files, are fruit of the poisonous tree and should be suppressed. United States v. Six hundred Thirty-nine Thousand Dollars, 955 F.2d 712, 719 (D.C.Cir. 1992). The evidence was obtained in violation of the Fourth Amendment.

F. The same applies to any equivalent program.

The affidavit and the nature of the query described therein demonstrate that the government utilized either the BTMP or some equivalent program with the same parameters. Judge Leon's decision applies equally to any program equivalent to BTMP: "I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy." Klayman, 957 F. Supp. 2d at 32.

To the extent the government claims the instant database differs in *material* respects from the BTMP, defendant requests discovery and an evidentiary hearing to allow the Court to determine the facts surrounding the database.

II. EVEN IF THE BTMP IS FOUND TO BE CONSTITUTIONAL, ITS USE IN THIS CASE WAS UNLAWFUL AND THUS PER SE AN UNREASONABLE SEARCH.

In Klayman, the government admitted there were legal limits to use of the BTMP database (at 15):

> The FISC orders governing the Bulk Telephony Metadata Program specifically provide that the metadata records may be accessed only for counterterrorism purposes (and technical database maintenance). Holley Decl. ¶ 8; Shea Decl. ¶ 30. Specifically, NSA intelligence analysts, without seeking the approval of a judicial officer, may access the records to obtain foreign intelligence information only through "queries" of the records performed using "identifiers," such as telephone numbers, associated with terrorist activity.

The parameters of the program are still quite murky. But the above admissions in Klayman indicate that the relevant FISC orders governing the program mandate that only "identifiers" or telephone numbers *associated with terrorism* can be utilized for queries. Simply put, the orders state that an agent can only input and query a telephone number associated with terrorism.

In this case, the agent input Sheikhi's business number from his car. There is no claim that this telephone number was or is associated with terrorism. Therefore, on its face, utilization of this telephone number violated the government's own orders concerning use of the BTMP.

Thus, even if the BTMP program as a whole is held to be constitutional, its usage *in this case* violated the orders

governing and permitting the program. In such event, the action remains an unwarranted and illegal search as to Mr. Hassanshahi. The resulting evidence from the computer should still be suppressed.

III. DEFENDANT IS ENTITLED TO DISCOVERY TO LEARN THE PARAMETERS AND ORDERS GOVERNING THE INSTANT DATABASE TO TEST WHETHER THE ORDERS WERE FOLLOWED AND THE QUERY WAS LAWFUL.

If the government contends the subject database was not the BTMP, Mr. Hassanshahi is entitled to discovery and an evidentiary hearing to determine the facts surrounding the database and the rules governing its use. It may be that the FISC order or some other order creating the database was not followed, rendering the query an unreasonable search.

Or it may be there was no authority at all to create and maintain the subject database. As to BTMP, the government claims authority from FISA and orders from the FISC courts. What, if anything, was the authority to create, maintain and query the bulk telephony database utilized in this case? Depending on the answer, the government may be on weaker ground with the actual database than with BTMP.

IV. SEPARATELY, THE EVIDENCE SHOULD BE SUPPRESSED BECAUSE THE GOVERNMENT LACKED REASONABLE SUSPICION TO CONDUCT THE FORENSIC COMPUTER EXAMINATION IN LOS ANGELES.

Under Ninth Circuit precedent applicable to the Los Angeles International Airport (LAX), where the subject computer search was conducted/initiated, the type of comprehensive forensic examination of the computer undertaken here can be conducted only upon "reasonable suspicion" of criminal activity. United States v. Cotterman, 709 F.3d 952 (2013). This is the same "articulable suspicion" needed to stop and frisk an individual on the street. The government's affidavit does not support reasonable suspicion prior to the LAX computer search.

A. The nature of the computer search conducted in this case.

The LAX computer search was not simply a "turn on and look" search. The government seized the computer and related data materials and kept them for weeks. During this time, the government broke or bypassed any password protection on the computer. The government then systematically identified, copied and examined each and every file, letter, email, photo, record or other data of any kind on the device.

In Cotterman, the government seized Cotterman's laptop while he was returning to the United States through the US-Mexico border. 709 F.3d at 952. The government shipped the computer to an electronic laboratory 170 miles away from the border and kept it for many days. There, the government

conducted a comprehensive forensic examination of the computer the electronic data thereon (hard drive). Through this examination, the government found child pornography and arrested Cotterman. The government failed to obtain a warrant for either the initial seizure of the computer at the border or the subsequent forensic examination. Cotterman moved to suppress the evidence obtained from the laptop on the grounds that it was an unlawful search. Id. at 956.

As a preliminary matter, the court noted there was no legal difference between the physical border with Mexico and "functional borders at airports such as Los Angeles (LAX). Id. The Court went on to reject the government's contention that no warrant or anything else was required for the search on the grounds that it was conducted at the border:

> Although courts have long recognized that border searches constitute a "historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained," *United States v. Ramsey*, 431 U.S. 606, 621, 97 S. Ct. 1972, 52 L. Ed. 2d 617 (1977), reasonableness remains the touchstone for a warrantless search. Even at the border, we have rejected an "anything goes" approach. *See United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (en banc).

Instead (at 956):

> Mindful of the heavy burden on law enforcement to protect our borders juxtaposed with individual privacy interests in data on portable digital devices, we conclude that, under the circumstances here, reasonable suspicion was required for the

forensic examination of Cotterman's laptop.

The Court distinguished between a "look see" (officers had the traveler boot up the computer and looked on the screen), which does not require any reasonable suspicion, and the forensic examination conducted on Cotterman's computer (and in the instant case). The latter implicates privacy concerns that go beyond a simple "quick look" at the border. As the court held (at 962):

> It is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here . . . To carry out the examination of Cotterman's laptop, Agent Owen used computer forensic software to copy the hard drive and then analyze it in its entirety, including data that ostensibly had been deleted. This painstaking analysis is akin to reading a diary line by line looking for mention of criminal activity—plus looking at everything the writer may have erased.
> . . .
> We are now presented with a case directly implicating substantial personal privacy interests. The private information individuals store on digital devices—their personal "papers" in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank [which may be searched at the border without heightened cause].
> . . .
> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can

> store over 200 million pages—the equivalent of five floors of a typical academic library.
>
> 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." U.S. Const. amend. IV. The express listing of papers "reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government."**
> . . .
> 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.

In Cotterman, the Ninth Circuit did not require a search warrant and probable cause for the forensic computer examination. But the court did require "reasonable suspicion" of wrongdoing before such an examination can be conducted (at 968):

> **We therefore hold that the forensic examination of Cotterman's computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment.**
> . . .
> Reasonable suspicion is defined as "a particularized and objective basis for suspecting the particular person stopped of criminal activity. This assessment is to be made in light of "the totality of the circumstances." "[E]ven when factors considered in isolation from each other are susceptible to an innocent explanation, they may collectively amount to a reasonable suspicion."

Under Cotterman, for the fruits of the computer search to be admissible, the government must have had a "reasonable suspicion" that Mr. Hassanshahi was involved in criminal activity *before* the LAX seizure

B. Reasonable suspicion under Cotterman

"Reasonable suspicion" requires "articulable facts" that criminal activity may be afoot. United States v. Sokolow, 490 U.S. 1, 7 (1989). The officer must have a "particularized and objective basis for suspecting legal wrongdoing." United States v. Arivizu, 534 U.S. 266, 273 (2002).

In Cotterman, the court found the government did have reasonable suspicion based on the following facts known to the government before seizing Cotterman's computer:

(a) Cotterman was returning from a vacation in Mexico.

(b) At the border, the Treasury Enforcement Communication System (TECS) returned a hit for Cotterman. The hit indicated

that Cotterman was a sex offender, convicted of multiple counts of sexual and lewd conduct upon a child and child molestation. 709 F.3d at 957.

(c) The border agent detained Cotterman and consulted the contact person listed on the TECS entry. Based on that conversation, the agents "believed the hit to reflect Cotterman's involvement in some type of child pornography." Id.

(d) The TECS hit reflected that Cotterman was a convicted child sex offender who traveled frequently outside the United States including to a country "associated with sex tourism".

(e) Cotterman had equipment with him that was associated with sex tourism.

The Court held, "Cotterman's TECS alert, prior child-related conviction, frequent travels, crossing from a country known for sex tourism, and collection of electronic equipment... gave rise to reasonable suspicion of criminal activity." Id. at 969.

C. In this case, the government lacked reasonable suspicion for the LAX computer seizure.

What facts did the agent actually have concerning Shantia Hassanshahi before he ordered the LAX computer seizure and search?

1. No informant had identified or even named Mr. Hassanshahi in any context. No one had suggested the involvement of any California-based person.

2. Sheikhi was suspected of soliciting a purchase of electrical equipment.

3. Calls had been placed to/from an 818-area code Google telephone number possibly associated with Mr. Hassanshahi to a number associated with Sheikhi, but:

(a) The contents of the calls were unknown.

(b) It was unknown whether either Sheikhi or Mr. Hassanshahi actually participated in the calls as opposed to some other persons with access to the phone account(s).

(c) The calls could have been placed from/to anywhere in the world.

(d) There is no evidence to suggest the calls were other than innocuous.

(e) The date/time/duration of the calls was either unknown or not specified in the affidavit.

4. Mr. Hasshanshi had/has no criminal record.

5. An email account possibly associated with Mr. Hassanshahi had been accessed from an IP address showing in Iran, however:

(a) There was no evidence Mr. Hassanshahi himself accessed the account as opposed to someone else with the password.

(b) The account could have been accessed through a VPN meaning the location of the use was unknown.

(c) There was no evidence of any emails between Mr. Hassanshahi or Sheikhi or anyone else involved in criminal activity.

6. Mr. Hassanshahi was indeed returning to Los Angeles from Iran in January 2012, but there is nothing unusual about this in and of itself.

7. Several telephone calls had been placed from the 818 number to the same number in Iran in September 2011, however:

(a) The government does not contend these calls were to Sheikhi or to Sheikhi's telephone number.

(b) There is no evidence of any criminal activity associated with these calls.

The government's "strongest" grounds of suspicion may be summarized as follows:

A. Mr. Sheikhi was suspected of violating or trying to violate the Iran trade regulations.

B. Telephone calls, contents unknown and participants undeterminable, had been placed to/from a number associated with Mr. Hassanshahi to a number associated with Mr. Sheikhi.

This simply does not constitute reasonable suspicion. That telephone calls were placed, alone, simply does not point towards criminal conduct on the part of Mr. Hassanshahi.

"Reasonable suspicion" is the same standard as is necessary for a police officer to "stop and frisk" a suspect on the street (a so-called Terry stop). The facts against Mr. Hassanshahi fall far short of any standard for a Terry stop.

By analogy to a standard drug case, the standard for the seizure and search of Mr. Hassanshahi’s personal computer is akin to a "stop and frisk" of each person coming in contact with a suspected drug dealer. Under the government's theory in this case, if calls are placed from telephone number X to/from a suspected drug dealer, then everyone associated with number X can be stopped and frisked by the police at the next

opportunity. For example, if telephone number X is at a house, then the police can wait outside the house and stop and frisk everyone who resides at the house on the grounds that these residents could have placed telephone calls from number X to the drug dealer. That is not the law.

The type of "contact" with Sheikhi alleged in this case is instead analogous to that considered in United States v. McCray, 148 F. Supp. 2d 379 (D.Del. 2001). In McCray, two experienced police officers patrolling an area known for drug and criminal activity observed defendant "huddling" with a suspected drug dealer. When the officers called to the persons, defendant started walking away from the scene "acting nervously" and took an object from his waistband and threw it away. 148 F. Supp. 2d at 383.

The officers stopped McCray, searched him, and found marijuana and crack cocaine, and thereafter obtained a confession. Id. at 384. McCray moved to suppress the results of the "stop and frisk" as not supported by reasonable suspicion.

The court agreed with McCray (at 386):

> In determining whether an officer's suspicion amounts to a reasonable suspicion, the court should consider the totality of the circumstances. *See United States v. Cortez*, 449 U.S. 411, 417, 66 L. Ed. 2d 621, 101 S. Ct. 690 (1981). Moreover, in determining whether a law enforcement officer had reasonable suspicion to justify a *Terry* stop, deference is given to the officer's conclusions based on the officer's experience. [citations] **"However, a mere 'hunch' or 'inchoate and unparticularized**

> **suspicion' cannot justify a stop and frisk under Terry.**" *Id.* at *4 (quoting *Brown*, 159 F.3d at 149). "**Instead, the officer must have a particularized and objective basis for believing that the particular person is suspected of criminal activity.**" *Id.* Applying these standard to McCray's case, the court concludes that Officers Muniz and Prado did not have a particularized and objective basis that would establish reasonable suspicion and, thus, justify their stop of McCray on August 14, 2000.
> . . .
> Even if the Bellflower was standing with Wallace and McCray, the officers still did not have a reasonable suspicion to believe that a drug transaction was occurring.. . . the one fact upon which both officers agreed is that neither saw anything pass between any of the individuals' hands. In this case, the officers maintain that they were suspicious that a drug transaction was taking place, yet they never saw the parties exchange anything. Observing two individuals who are possibly standing near a known loiterer, even one described as being involved in narcotics activity, without more, merely constitutes an "inchoate and unparticularized suspicion," and cannot justify a *Terry* stop.
>
> The court finds guidance in a *Washington v. Gilmore*, 1998 U.S. Dist. LEXIS 17309, No. C-97-4062 PJH, 1998 WL 774629 (N.D. Cal. Oct. 30, 1998), a civil rights case that arose out of a *Terry* stop. [9] In *Gilmore*, the court held that a police officer did not have reasonable suspicion of narcotics activity in a case that is factually similar to McCray's. *Id.* at *7. Officer Gilmore alleged that the defendant made "furtive gestures" like closing her fists and placing her hands towards her chest while in an automobile with a known drug dealer. *Id.* Even considering the defendant's proximity to a known drug dealer and the high crime area, the court held that the officer's observations established no more than an

> "'inchoate and unparticularized suspicion or hunch' that the Supreme Court has found insufficient to support a finding of 'reasonable suspicion.'" *See Id.* Moreover, the court found that the officer described no "objective manifestation" that Gilmore was or was about to be engaged in criminal activity.

Again, the standard for a Terry stop is the same as for the computer seizure and search in this case. Analogies can be drawn to McCray and to the Gilmore case cited therein. In both cases, the defendant is observed in close proximity and obviously communicating with a known drug dealer in a high-crime/drug area. But specific criminal activity, such as passing money or a package, is not observed. The defendant's proximity/communication with a known or suspected criminal is not enough to cast reasonable suspicion.

Here, putting the government's evidence in the best light, prior to the search the government had reason to believe Mr. Hassanshahi had communicated with Mr. Sheikhi, who *arguendo* was suspected of criminal activity. But even if Mr. Hassanshahi communicated with Sheikhi, which is unprovable, the absence of any indication of content does not afford a basis for a reasonable suspicion of wrongdoing.Otherwise, everyone who telephoned Mr. Sheikhi would be subject to a search.

CONCLUSION

All evidence obtained from the seizure of the computer at LAX and subsequent search and further fruits should be suppressed. If the evidence in the record is insufficient for the Court to determine the source of the information regarding

telephone numbers referenced in the Government's complaint, then the Court should order the production of discovery and conduct a hearing to allow the defense to probe the nature, parameters and rules governing the telephony database relied upon in this case.

DATED: March 27, 2014

[ORAL ARGUMENT REQUESTED]

John Pierce, Esq.
Themis PLLC
2305 Calvert Street, NW
Washington, DC 20008

/s/ John Pierce
John Pierce

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 March 27, 2014 and via the electronic filing system.

/s/ John Pierce
John Pierce