

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

2012 AUG 16 PM 2:06

In the Matter of the Search of

HTC Motorola 4G MyTouch Android Cellular Phone  
Model # PD15100  
Serial # SH0CCRM05776

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

MAGISTRATE CASE NO: 12 MJ 3058

I Sean Downey being duly sworn depose and state:

I am a Special Agent with U.S. Homeland Security Investigations and have reason to believe that on the property or premises known as:

**See Attachment A, which is attached and incorporated herein,**

in the Southern District of California

there is now concealed a certain person or property, namely

**Fruits, instrumentalities, and evidence of and concerning violations of 50 U.S.C. § 1701, et seq., 18 U.S.C. §§ 554 and 371, 18 U.S.C. § 1956(a)(2), and 18 U.S.C. § 1512, more fully described in Attachment B, which is attached and incorporated herein,**

which is

**Property and electronic data that constitutes evidence of the commission of a criminal offense, and which is and has been used as the means for committing a criminal offense**

concerning violations of Title 50, United States Code, Section 1701, et seq.

The facts to support a finding of Probable Cause are as follows:

**See attached affidavit of HSI Special Agent Sean Downey, which is attached and incorporated herein**

Continued on the attached sheets and made a part thereof.  Yes  No

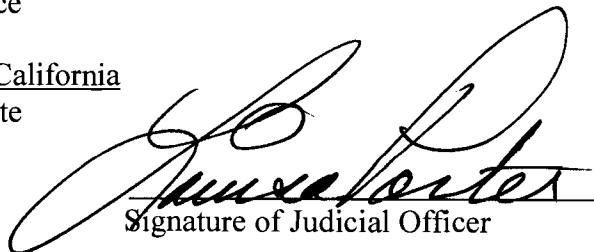
  
Signature of Affiant

Sworn to before me, and subscribed in my presence

August 16, 2012  
Date

San Diego, California  
City and State

Louisa S. Porter, U.S. Magistrate Judge  
Name and Title of Judicial Officer

  
Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR SEARCH WARRANT**

I, Sean Downey, Special Agent, United States Homeland Security Investigations (HSI), being duly sworn, state:

1. This affidavit is in support of an application by the United States of America for a search warrant for the following cellular telephone: an HTC Motorola 4G MyTouch Android smart phone with serial number SH0CCRM05776 and model number PD15100 (**subject phone**). I seek authority to search this phone, as described in Attachment A, for items that constitute evidence, fruits, and instrumentalities of violations of federal criminal law, namely, conspiracy to export goods to Iran without a license, in violation of the International Emergency Economic Powers Act ("IEEPA") (50 U.S.C. § 1701 et. seq., 31 CFR 560.204, 560.203); conspiracy to smuggle goods from the United States (18 U.S.C. §§ 554 and 371); money laundering (18 U.S.C. § 1956(a)(2)); and obstruction of justice (18 U.S.C. § 1512).

2. My knowledge of the facts alleged in this affidavit arises from my training and experience, my personal observations, my participation in the federal investigation described herein, my conversations with other law enforcement agents involved in this investigation, my interviews of U.S. manufacturers, and my review of records obtained during this investigation. Because this affidavit is submitted for the limited purpose of securing a search warrant as described herein, it does not include every fact known to me concerning the investigation.

**EXPERIENCE AND TRAINING**

3. I am an HSI Special Agent and have been so employed since October 2010. I am currently assigned to conduct investigations involving illegal exports. My current responsibilities include investigating the illegal transfer and export of commodities, information,

and services from the United States, which are regulated by the United States Departments of State, Commerce, and the Treasury. While working as a Special Agent with HSI, I have been involved in investigating violations of federal law, including the illegal transfer and export of commodities from the United States, money laundering, and fraud against the government.

**LEGAL BACKGROUND ON U.S. SANCTIONS AGAINST IRAN**

4. The International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. § 1701 et seq., authorizes the President of the United States of America to deal with unusual or extraordinary threats to the national security, foreign policy, and economy of the United States. Specifically, 50 U.S.C. § 1702 provides, in pertinent part, “At the times and to the extent specified in section 1701 of this title, the President may, under such regulations as he may prescribe, by means of instructions, licenses, or otherwise (A) investigate, regulate, or prohibit (i) any transactions in foreign exchange.”

5. On or about March 15, 1995, pursuant to IEEPA, the President issued Executive Order 12957 (“EO 12957”), finding that the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. On that same date, the President declared a national emergency to deal with that threat. On or about May 6, 1995, the President issued Executive Order 12959 (“EO 12959”) to take additional steps to deal with the unusual and extraordinary threat presented by Iran to the national security, foreign policy, and economy of the United States.

6. Effective May 7, 1995, EO 12959 prohibited, among other things: (1) the unauthorized exportation from the United States to Iran, or the financing of such exportation, of any goods, technology, or services, except publications and donations of articles intended to relieve human suffering; and (2) any transaction by any United States person or within the

United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions contained in the Iranian Transactions Regulations (“ITR”), codified in part at 31 C.F.R. 560.204. Section 560.204 of the ITR prohibits the unauthorized exportation, reexportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran or the Government of Iran.

7. The acts prohibited by IEEPA are codified at 50 U.S.C. § 1705, which provides, in pertinent part:

(a) Unlawful acts. It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this title.

(b) . . .

(c) Criminal penalty. A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of, an unlawful act described in subsection (a) shall, upon conviction, be fined . . . , or if a natural person, may be imprisoned for not more than 20 years, or both.

**FACTS SUPPORTING PROBABLE CAUSE  
TO SEARCH THE SUBJECT ACCOUNT**

8. Mohammad Reza NAZEMZADEH is in the United States on an H1-B visa. He is a research fellow affiliated with the University of Michigan’s Neurology Department. On February 15, 2011, he signed an I-485 Application to Register Permanent Residence or Adjust Status under penalty of perjury. On the form, he indicated that he did not “intend to engage in the United States in . . . any activity to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information.”

9. On August 12, 2011, NAZEMZADEH emailed a San Diego company that sells new and used medical device equipment to request pricing information on a brain array coil used

in MRI machines. The company knew from prior correspondence with NAZEMZADEH that he was seeking to buy equipment for use Iran. The company notified HSI and agreed to introduce an undercover agent (UCA) to NAZEMZADEH as a company salesperson. On August 15, 2012, the UCA replied to NAZEMZADEH's inquiry.

10. On August 16, 2011, the UCA made a recorded phone call to NAZEMZADEH at (248) 269-3570, the phone number assigned to the **subject telephone**. During that call, NAZEMZADEH identified himself and the UCA introduced him/herself as the person who had emailed NAZEMZADEH regarding the coil. NAZEMZADEH and the UCA discussed pricing for the MRI coil and NAZEMZADEH indicated that the customer wanted the coil as soon as possible. NAZEMZADEH asked the UCA to prepare a pro forma invoice and said that the coil should be shipped to Hospital Equipment Services (HES) in the Netherlands because it was "safer." NAZEMZADEH told the UCA that HES sometimes re-shipped items to other customers and that HES charged its customers 10% to purchase and transship items. When pressed by the UCA, NAZEMZADEH acknowledged that the coil he wanted shipped to HES was for a customer in Iran. The UCA told NAZEMZADEH that, although the UCA was not an expert on export laws, s/he understood that medical equipment could not be shipped to Iran without a license, even if it was trans-shipped through a third country. The UCA then asked NAZEMZADEH if he wanted the UCA to apply for an export license. NAZEMZADEH, after initially saying it was the UCA's decision (which the UCA rejected), said that it would be better to sell the coil to HES, who would pass it along to the Iranian customer, because the customer was in a rush. NAZEMZADEH said that they would "maybe" apply for a license for future deals. During this conversation, NAZEMZADEH repeatedly referenced "OFAC" and the embargo against Iran. (As discussed above, OFAC administers licenses for exports to Iran.)

11. On August 18, 2011, the UCA emailed NAZEMZADEH a \$21,400 price quote for the coil. On August 22, 2011, an HES employee named Tijn Simons emailed the UCA and cc'd NAZEMZADEH and Kayvan Hashemi (K. Hashemi). Simons attached a copy of a wire statement showing the deposit of \$21,400 into a San Diego undercover account. On August 24, 2011, HSI confirmed the deposit.

12. After receiving payment, HSI obtained a fake UPS tracking number. On September 6, Olga Schutte, an HES employee, emailed Mohammed Hashemi (M. Hashemi) and the UCA that UPS Netherlands had said the package containing the coil was lost and that the U.S. shipper needed to contact the local UPS office. On September 7, the UCA received an email written in Farsi from Homayoun. The UCA forwarded it to NAZEMZADEH. The next day, the UCA emailed NAZEMZADEH, Schutte, K. Hashemi, M. Hashemi, and Mohsen Homayoun and told them that UPS said that the package was stopped by Dutch Customs at the request of U.S. Customs and that representatives would be in touch.

13. On September 15, 2011, an HSI agent using his real name and title emailed the UCA details regarding a meeting to discuss the export of the brain array coil and asked the UCA to collect all paperwork pertaining to the transaction. The UCA forwarded the agent's email to NAZEMZADEH, Simons, and Schutte.

14. That day, the UCA and NAZEMZADEH had a recorded phone call that, according to caller identification, NAZEMZADEH made from the **subject phone's** number. During the call, NAZEMZADEH repeatedly asked the UCA not to mention his involvement to the authorities because he was Iranian and insisted that the transaction was legal. NAZEMZADEH acknowledged having told the UCA that the coil was going to Iran and told the UCA:

Just tell that, you sold that item to some company in the Netherlands, and you have the request so you're, you issued pro forma form for them and they sent money from the bank account to you, everything is legal between you[r] two companies . . . . [T]here's nothing to do with Iran. You actually have sold that coil to one company in Netherland, ok?

15. When the UCA asked, "So, you want me to not to tell them about you, is that what you want?" NAZEMZADEH replied, "Yes, exactly." When the UCA asked what to do about the emails listing NAZEMZADEH and the other Iranian names, NAZEMZADEH suggested, "What about, because [Schutte] has called you several times, maybe tell them that you've got the order by your phone . . . . [and she] has been in correspondence with you." NAZEMZADEH also suggested that, if necessary, the UCA could "remove all the Iranian names from the emails." Later, he asked the UCA, "So can I ask you to just show them the emails between you and Olga?"

16. During this call, NAZEMZADEH said, "I'm so afraid that Homeland Security would just get fired me [sic] from the country because something stupid I've done." Later, he said, "HES company would actually act wisely because they're in trouble, too, against US sanctions."

17. On December 15, 2011, a grand jury sitting in the Southern District of California returned an indictment charging NAZEMZADEH with one count of Obstruction of Justice, in violation of 18 U.S.C. § 1512(b)(3). An arrest warrant was also issued for NAZEMZADEH's arrest. On or about January 18, 2012, HSI agents arrested NAZEMZADEH in Michigan. At that time, agents seized NAZEMZADEH's phone, which is the **subject phone**. The **subject phone** has been in the custody of HSI-San Diego since.

18. On or about May 23, 2012, NAZEMZADH's counsel provided written consent to HSI to search the **subject phone**. During the time that HSI agents had consent to search the phone, they determined that the **subject phone** was assigned phone number (248) 269-3570.



HSI was also able to search the **subject phone's** Subscriber Identity Module (SIM) card and micro-SIM card. (SIM cards are portable memory chips used in some cellular telephones.<sup>1</sup>) Evidence found on these cards include a May 2011 invoice from a U.S. company that listed HES as the buyer and over a dozen photographs of medical equipment.

19. HSI, however, was unable to search the phone itself because the phone was password-protected and the passwords provided by NAZEMZADEH's counsel did not match. HSI contacted Google for assistance to unlock the phone and advised Google that HSI had written consent to search the phone, but Google said that they would only unlock the phone with a search warrant.

20. On the evening of August 14, 2012, NAZEMZADH's counsel provided written notice that NAZEMZADEH had revoked his consent for HSI to search the phone.

21. Based on the foregoing, I submit that there is probable cause to search the **subject phone**.

### CELL PHONE SEARCH WARRANT METHODOLOGY

#### Procedures For Electronically Stored Information

22. It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access

---

<sup>1</sup> See [http://wiki.answers.com/Q/What\\_is\\_a\\_SIM\\_card](http://wiki.answers.com/Q/What_is_a_SIM_card).



their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in “flight mode” which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.


23. Following the issuance of this warrant, I will collect the subject cellular telephone and subject it to analysis. All forensic analysis of the data contained within the telephone and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

24. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within ninety (90) days, absent further application to this court.

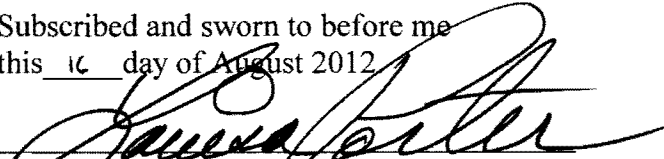
### **CONCLUSION**

25. Based on the foregoing, I submit that there is probable cause to believe that the items identified in Attachment B have been used in the commission of a crime and constitute

evidence, fruits, and instrumentalities of violations of 50 U.S.C. § 1701 et. seq., 31 CFR 560.204, 560.203; 18 U.S.C. §§ 554 and 371; 18 U.S.C. § 1956(a)(2); and 18 U.S.C. § 1512; and that the foregoing will be found on the cellular telephone to be searched, as identified in Attachment A.

  
Special Agent Sean Downey  
U.S. Homeland Security Investigations

Subscribed and sworn to before me  
this 16 day of August 2012.

  
HON. LOUISA S. PORTER  
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The cellular telephone to be searched is:

HTC Motorola 4G MyTouch Android Cellular Phone  
Model # PD15100  
Serial # SH0CCRM05776

currently in the custody of Homeland Security Investigations at 185 West F. St, San Diego, CA 92101.

ATTACHMENT B

The evidence to be searched for and seized pertains to violations of 50 U.S.C. § 1701 et. seq., 31 CFR 560.204, 560.203; 18 U.S.C. §§ 554 and 371; 18 U.S.C. § 1956(a)(2); and 18 U.S.C. § 1512, and is described as follows:

- a. Communications or data—such as emails, text messages, photographs, audio files, or videos—tending to indicate efforts to acquire technology or other goods or services for export or re-export to Iran;
- b. Communications or data tending to identify other facilities, storage devices, or services—such as email addresses, IP addresses, phone numbers—that may contain electronic evidence tending to demonstrate efforts to acquire technology or other goods for export or re-export to Iran;
- c. Communications or data tending to demonstrate knowledge of laws related to exports and re-exports to Iran;
- d. Communications or data, including but not limited to contacts and call history, tending to identify co-conspirators or criminal associates;
- e. Communications or data tending to identify travel to or meetings with others involved in acquiring technology or goods for export or re-export to Iran; and
- f. Communications or data tending to identify the user, or persons with dominion and control over the subject phone, including email, text messages, photographs, and video.