MARK RUMOLD (SBN 279060)
mark@eff.org
DAVID GREENE (SBN 160107)
NATHAN D. CARDOZO (SBN 259097)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
HANNI FAKHOURY (SBN 252629)
JAMIE L. WILLIAMS (SBN 279046)
ANDREW CROCKER (SBN 291596)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Plaintiff
Human Rights Watch

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

HUMAN RIGHTS WATCH,

Plaintiff,

v.

DRUG ENFORCEMENT ADMINISTRATION, *et al.*,

Defendants.

Case No: 2:15-cv-2573-PSG-JPR

DECLARATION OF MARK RUMOLD FILED IN SUPPORT OF PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Date: August 17, 2015
Time: 1:30 p.m.
Courtroom 880 – Roybal
Hon. Philip S. Gutierrez

I, MARK RUMOLD, hereby declare:

1. I am an attorney of record for plaintiffs in this action and a member in good standing of the California State Bar. I am admitted to practice before this Court. I have personal knowledge of the matters stated in this declaration and if called upon to do so I am competent to testify to all matters set forth herein.

2. Attached hereto as Exhibit 1 is a true and correct copy of the following document: Affidavit of Joshua J. Akronowitz, in Support of Criminal Complaint, filed in *United States v. Hassanshahi*, 1:13-cr-00274-RC (D.D.C. January 9, 2013) (ECF No. 1-1).

3. Attached hereto as Exhibit 2 is a true and correct copy of the following document: Affidavit of Joshua J. Akronowitz, filed in *United States v. Hassanshahi*, 1:13-cr-00274-RC (D.D.C. July 10, 2014) (ECF No. 37-1).

4. Attached hereto as Exhibit 3 is a true and correct copy of the following document: The United States' Reply to Defendant's Response to the United States' February 25, 2015 Memorandum, filed in *United States v. Hassanshahi*, 1:13-cr-00274-RC (D.D.C. April 29, 2015) (ECF No. 58).

5. Attached hereto as Exhibit 4 is a true and correct copy of the following document: Brad Heath, *U.S. secretly tracked billions of calls for decades*, USA Today (April 8, 2015). This article is available online at: http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-

operation/70808616/.

6. Attached hereto as Exhibit 5 is a true and correct copy of the following document: Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, The Intercept (Aug. 25, 2014). This article is available online at: https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.

Dated: July 27, 2015

Respectfully submitted,

s/ Mark Rumold
MARK RUMOLD
DAVID GREENE
NATHAN D. CARDOZO
LEE TIEN
KURT OPSAHL
HANNI FAKHOURY
JAMIE L. WILLIAMS
ANDREW CROCKER

ELECTRONIC FRONTIER FOUNDATION

Counsel for Plaintiff Human Rights Watch

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States District Court for the Central District of California by using the Court's CM/ECF system on July 27, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the Court's CM/ECF system.

Dated: July 27, 2015

s/ Mark Rumold
MARK RUMOLD

Exhibit 1

Exhibit 1

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

SHANTIA HASSANSHAHI
also known as SHANTIA HASSAN SHAHI
also known as SHAHI
also known as SHANTIA HAAS
also known as SEAN HAAS

and

HASSTON, INC.

I, Joshua J. Akronowitz, being first duly sworn, depose and state as follows:

AFFIANT'S BACKGROUND

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI") and have been so employed since September 2007. I am a graduate of the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. At FLETC, I was trained in, among other things, criminal investigative techniques. I have participated in criminal investigations involving, among other things, the illegal export of goods from the United States. I have received formal training in the laws and regulations relating to the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C §§ 1701-1706, and the Iranian Transactions Regulations ("ITR"), 31 C.F.R. Parts 560.203 and 560.204. I have conducted and participated in investigations of the above listed laws and regulations.

2. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. In addition, I have received information from other federal law enforcement officials. I also have reviewed documents obtained during the course of the investigation. The statements contained in this affidavit are based on my own observations and review of documents, or reliable information provided to me by other law enforcement personnel and by private citizens. This affidavit is being submitted for the limited purpose of supporting a criminal complaint. I am setting forth only those facts and circumstances necessary to establish probable cause for the issuance of the requested complaint. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

PURPOSE OF AFFIDAVIT

3. This affidavit is in support of a criminal complaint charging **SHANTIA HASSANSHAHI, also known as SHANTIA HASSAN SHAHI, also known as SHAHI, also known as SHANTIA HAAS, also known as SEAN HAAS ("HASSANSHAHI"); and HASSTON, INC.,** with having violated IEEPA (50 U.S.C. § 1705) by conspiring to export goods to Iran without first having obtained the necessary export license.

EXPORT CONTROL LAWS AND REGULATIONS

4. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C §§ 1701-1706, authorizes the President of the United States ("the President") to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy or economy of the United States when the President declares a national emergency with respect to that threat. Pursuant to the authority under the IEEPA, the President and the executive branch have issued orders and regulations governing and prohibiting certain transactions with Iran by U.S. persons or involving U.S.-origin goods.

5. Beginning with Executive Order No. 12170, issued on November 14, 1979, the President has found that "the situation in Iran constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United States and … declare[d] a national emergency to deal with that threat."

6. On May 6, 1995, the President issued Executive Order No. 12959, adopting and continuing Executive Order No. 12170 (collectively, the "Executive Orders"), and prohibiting, among other things, the exportation, reexportation, sale, or supply, directly or indirectly, to Iran of any goods, technology, or services from the United States or by a United States person. The Executive Orders authorized the United States Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the ITR, implementing the sanctions imposed by the Executive Orders.

7. The Iranian Transactions Regulations ("ITR"), 31 C.F.R. Part 560, generally prohibit any person from exporting or causing to be exported from the United States any goods, technology, or services without having first obtained a validated export license from the United States Department of the Treasury, Office of Foreign Assets Control ("OFAC"), which is located in the District of Columbia. The ITR imposes, among others, the following prohibitions:

> Section 560.203 - Prohibition of any Transaction to Evade or Avoid the Embargo and any Attempt to Violate the Embargo:

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 this part is hereby prohibited.

Section 560.204 - Prohibition of any Sale or Supply of any Goods, Technology, Services to Iran or the Iranian Government:

Except as otherwise authorized [by a license issued by OFAC], the 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 is prohibited, including the exportation, reexportation, sale, or supply of any goods, technology, or services to a person in a third country undertaken with knowledge or reason to know that:

(a) Such goods, technology, or services are intended specifically for supply, transshipment, or reexportation, directly or indirectly, to Iran or the Government of Iran . . .

Section 560.314 – United States Person; U.S. person:

The term *United States person* or *U.S. person* means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

8. On October 15, 2007, the IEEPA was amended to include a criminal conspiracy provision and an increased fine. Title 50, United States Code, Section 1705 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 chapter.

* * *

(c) Criminal penalty

A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act described in subsection (a) of this section shall upon conviction, be fined not more

than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both.

FACTUAL BASIS FOR PROBABLE CAUSE

9. It is my experience and the experience of law enforcement officers with whom I work, that individuals and companies attempting to circumvent the current United States embargo against Iran will export or cause to be exported goods and technology to companies located in non-embargoed countries for transshipment to end-users in Iran.

10. Since August 2011, HSI Washington, DC ("HSI-DC") has been investigating the attempted procurement of "protection relays" by individuals associated with or attempting to do business with the Government of Iran, specifically the Ministry of Energy, for apparent use in the Iranian national electrical power grid. Protection relays are complex electromechanical devices that are incorporated into and designed to calculate operating conditions on electrical circuits. Protection relays are generally intended to trip circuit breakers when a fault in the circuit is detected, for the primary purpose of preventing damage, malfunctioning, or "blackouts" of an electrical circuit or power grid.

11. In September 2011, as part of an ongoing criminal investigation, HSI-DC identified a company in Iran (hereinafter referred to as "HIMAFAN") involved in the procurement and exportation of protection relays from different companies located in the U.S. and Canada. HSI-DC determined that two individuals, an "M. Sheikhi" and "Mohammad Reza BABAEI", both Iranian nationals, were the primary agents involved in the operation of HIMAFAN's procurement and export activities. HSI-DC's investigation also revealed that over the course of several years, beginning in and around 2009, "Sheikhi", on behalf of HIMAFAN, procured protection relays from **HASSTON, INC. ("HASSTON")**, a company incorporated in California and located at 1636 Castlehill Ct., Westlake Village, CA 91361, through its owner **SHANTIA HASSANSHAHI**, **also known as SHANTIA HASSAN SHAHI, also known as SHAHI, also known as SHANTIA HAAS, also known as SEAN HAAS ("HASSANSHAHI")** (DOB: 4/18/1955), an Iranian-born U.S. Citizen residing in California, for export to Iran in violation of the IEEPA and ITR.

Background

12. 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.

13. 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:

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.

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.

14. 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:

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.

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.

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.

Identification and Border Search of HASSANSHAHI

15. 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.

16. 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

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.

17. 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.

18. 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.

19. 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.

20. 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:

- A copy of the Articles of Incorporation for **HASSTON**, indicating that it was incorporated on March 16, 2009, and is located in Westlake Village, CA. According to the California Secretary of State's website, **HASSANSHAHI** is **HASSTON**'s registered agent. Notably, the business address provided for **HASSTON** was also **HASSANSHAHI**'s then home address. Moreover, while **HASSTON**'s public website indicates that it is "under construction," open source information indicates that **HASSTON**'s domain name is registered to **HASSANSHAHI**.

- A document entitled "Memorandum of Understanding and Cooperation" dated on or about December 31, 2009, regarding HIMAFAN, signed by **HASSANSHAHI** and "BABAEI"

- The first Article, entitled "Article 1: The Parties to the Memorandum" provided the date of the agreement being entered into of December 31, 2009. The parties listed were **HASSANSHAHI** (referred to as 2nd party) with an Iranian address, which I later identified as belonging to his Iranian company used to facilitate the arrival of these protection relays into Iran (hereinafter referred to as "KIAN DAY"), and HIMAFAN (referred to as the 1st party) also with an Iranian address. The second article, entitled "Article 2: The Objective of Memorandum" included the stated goal was to contact the U.S./Canadian company (hereinafter referred to as "COMPANY A") and to provide items needed by the 1st Party for sale in the country. The fourth article, entitled, "Article 4: The Undertakings by the 1st Party" explained the following in three distinct bullets:

    a. "Providing guarantees needed for entering into contracts with the 3rd party companies for the sale of items purchased from

COMPANY A by the 2nd party."

b. "Receipt of payments for the purchased items from the 3rd party company and paying the 2nd party for payment to COMPANY A in Canada."

c. "Clearance of goods shipped by the 2nd party through the Customs in Armenia and their shipment to and clearance in Tehran."

The fifth article, entitled, "Article 5: The Undertakings by the 2nd party" stated, "Procuring equipment (with payments from the First Party to be received through agreements with the 3rd party company) requested by the 1st party from COMPANY A in Canada and delivering them to the representative of the 1st party at the Customs in Armenia.

- Contact information for a company called HIMAFAN located and doing business in Tehran, Iran. Open source information found on the Internet indicates that HIMAFAN is "a leading provider of products, systems, and services of the Transmission and Distribution industry . . . ." Notably, my review of the call log records for telephone number (818-971-9512)—serviced by Google and subscribed to by **HASSANSHAHI**—appeared to show that HIMAFAN's known business telephone number had been used to place a number of calls to **HASSANSHAHI**.

- Hundreds of e-mails sent and received by **HASSANSHAHI** in furtherance of the business of **HASSTON** and KIAN DAY. When conducting business through **HASSTON**, **HASSANSHAHI** frequently used the following e-mail signature block, identifying **HASSANSHAHI** as the President of **HASSTON** and listing shantia34@gmail.com as the contact e-mail address for him in that capacity:

  Shantia Hassanshahi
  Hasston, Inc..-President
  (805) 857-4246 - U.S. Office
  (213) 417-4086 - VOIP Phone
  (310) 651-9680 - US Fax
  +44 (1273) 311-461 UK Office3
  shantia34@gmail.com <mailto:shantia34@gmail.com>

- When conducting business through KIAN DAY, **HASSANSHAHI** frequently used the following e-mail signature block, identifying **HASSANSHAHI** as the President of KIAN DAY located in Tehran, Iran:

  Shantia Hassanshahi
  Kianday, Inc. - President

Phase I Block A4 Entrance 11, Suite 419
Ekbatan, Tehran - Zip Code 13947-43876 Iran
+98(21) 4464-6324 - Office
+98(935) 4464-6324 - Mobile
+44(1273) 311-461 - UK Office

22. Moreover, the following documentation was found on **HASSANSHAHI**'s laptop computer, establishing that in 2009, **HASSANSHAHI**, through **HASSTON**, had purchased approximately $6,000,000 worth of goods from COMPANY A (in Canada) that were exported to Armenia and then transshipped to KIAN DAY in Iran.

- An e-mail **HASSANSHAHI** sent on June 28, 2009, attached to which was a pro forma invoice issued by Armandey, an Armenian company, to KIAN DAY in Tehran, Iran, bearing purchase order number "P-06102009," and identifying KIAN DAY and **HASSANSHAHI** as the intended recipients of the goods in Iran.

- Shipping records from COMPANY A in Canada, falsely indicating that the ultimate consignee and destination for the shipment was Armandey, in Yerevan, Armenia.

- 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.)

Date: September 5, 2011

Engineer Namjoo
Honorable Minister of Energy

RE: Procurement of Relays for Fars Regional Electric Company

Greetings,

You are respectfully informed that Fars Regional Electric Company called for bids for the purchase of protective relays for transmission lines in '88[1]. The purchasing documents and participation in the bid were handled by an intermediary company called Permayon.

It was agreed that Permayon Company would act as an intermediary between my company in the United States and Fars Regional Electric Company and that it would appear for the bid offer and proceed with providing the guaranties and financing of the project.

Unfortunately, after winning and entering into a contract in the amount of 1,250,000 United States dollars with Fars Regional Electric Company, the intermediary failed in its financial obligations, both when receiving the advance payment from the main client and when it had to make payments to me during the completion of the project so that I could pay the manufacturer, COMPANY A. To date, the sum of 500,000 dollars out of 1,000,000 dollars has been paid by the intermediary company. But given the obligations that I had and still do have to COMPANY A, the project payments had to be made in due time. In order to settle up with COMPANY A, I have made one payment of 200,000 dollars. I was given credit for three months by COMPANY A. Unfortunately, six months after the delivery of all items to the intermediary company and the main client, no payments have been made by the main client so that I can settle up the remaining 300,000 dollars with the manufacturer.

After many inquiries, the intermediary company stated that it is unable to pay what I am owed and sidestepped its obligations and pointed to Fars Regional Electric Company as being responsible for payments.

In a letter, Fars Regional Electric Company reassigned payment of 50 per cent of its debt to Tavanir Company. This was supposed to be paid by Tavanir by the end of the month of Mordad[2] of the current year, but that has not materialized as of now. The remaining 50% was supposed to be paid by Fars Regional Electric Company in the beginning of the month of Mehr[3] of the current year, but as of now, that also remains unclear.

---

[1] This Persian calendar year corresponds to the period from March 21, 2009 to March 20, 2010 (Translator's note.)
[2] This Persian calendar month refers to the period from July 23 to August 22, 2011 (Translator's note.)
[3] This Persian calendar month refers to the period from September 23 to October 22, 2011 (Translator's note.)

Considering the above, the losses and damages, my unfulfilled obligations to COMPANY A, I am left in a situation where it is feared that the manufacturer may bring a lawsuit against me in American courts for failure to act under obligations. And given that I am an Iranian and that these items are subject to sanctions and the fakeness of the end user, the worst will be expected.
In view of what has been stated, I ask your honor's favorable view and giving of instructions to persons in charge for a speedy settlement of the accounts with me.
I thank you very much in advance for your honor's attention.

Thank you,
Shantia Hassanshahi

- On September 5, 2011 HASSANSHAHI sent a letter similar to the one above to Tavanir Co., an Iranian company. This letter, like the one above, outlines the procurement of COMPANY A protection relays for the Iranian Fars Regional Electric Power Company using **HASSANSHAHI**'s U.S. company, **HASSTON**. In addition this letter also addresses the sanctions on Iran and the need to use fake end-users and Asian countries to divert their shipments. This letter appears below.[1] (The name of the company has been substituted with "COMPANY A" in the body of the letter below.)

[1] On September 19, 2011 **HASSANSHAHI** sent a letter to Iranian Minister or Energy Namjoo as a follow-up expressing most of the points as stated in the September 5, 2011

HASSTON

In the Name of God,

Date: September 5, 2011

Engineer Haeri
Honorable Chief Executive of Tavanir Company

RE: Procurement of Protective Relays for Fars Regional Electric Power Company

Greetings,

Respectfully, I would like to inform you that Fars Regional Electric Power Company called for bids for the purchase of protective relays for transmission lines in '88[1]. The purchasing documents and participation in the bid were handled by an intermediary company called Permayon. It was agreed that Permayon Company would act as an intermediary between my two companies–Hasston in the United States and Himafan Company in Iran–and Fars Regional Electric Power Company, and that it would appear for the bid offer and proceed with providing the guarantees and financing of the project.

Unfortunately, after winning and entering into a contract in the amount of 1,250,000 United States dollars with Fars Regional Electric Power Company, the intermediary company failed to act on its financial obligations, both when receiving the advance payment from the main client and when it had to make payments to me during the completion of the project so that I could pay the manufacturer, Company A. To date, the sum of 500,000 dollars from the manufacturer's sale price of 1,000,000 dollars has been paid by the intermediary company. But given the obligations that I had and still have towards Company A, it had been agreed that the project payments would be made in due time. In order to settle up, I personally have paid 200,000 dollars as a partial payment of the amount owed to Company A and because of my standing, I have obtained from Company A a deferral for three months. Unfortunately, six months after the delivery of all the items in the contract to the intermediary company and Fars Regional Electric Power Company, no payments have been made by the main client-

Address Redacted
[redacted] (805) 857-4246 - US Office
Address Redacted, CA 91361 [redacted] (310) 651-9680 - US FAX
[redacted] (213) 417-4086 – VOIP Phone
[redacted]@gmail.com

[1] This Persian calendar year corresponds to the period from March 21, 2009 to March 20, 2010 (Translator's note.)

HASSTON

so that I can pay the remaining 300,000 dollars to the manufacturer. It should be mentioned that I have to pay the entire amount that I owe to the manufacturer by October 2011 (That is, in less than 20 days.) If Company A is not paid by the said date, that company will probably begin to look into the address and information of the fake user in the Central Asian countries. This would mean giving away the diverted itineraries of the *High Tech* goods to our country!

After many inquiries, the intermediary company stated that it is unable to pay what I am owed and sidestepped its obligations and pointed to Fars Regional Electric Power Company as being responsible for payments.

In a letter, Fars Regional Electric Power Company reassigned the payment of 50 percent of the amount it owes to Tavanir Company. Tavanir was supposed to pay this by the end of the month of Mordad[2] of the current year at the latest, but that has not materialized as of now. The other portion of the amount owed to me was supposed to be paid by the Regional Electric Power Company in the beginning of the month of Mehr[3] of the current year, but based on the current information, that also remains unclear.

In consideration of the above, the losses and damages incurred, the waste of more than one month for travel to Iran – while leaving my company in the United States unattended – to appear in the Ministry of Energy to resolve this matter, I ask you to note that my unfulfilled obligations toward Company A puts me in a critical and worrisome situation where it is feared that the manufacturer may bring a lawsuit against me in American courts for breach of agreement. Since I am an Iranian and that these *High Tech* items are subject to sanctions and that the address and information of the end user is fake, the worst legal problems will be expected.

Based on what has been stated, I ask for your honor's favorable view and giving of instructions to persons in charge for a speedy payment of the total or at least 300,000 dollars of what is owed to me so that I pay the manufacturer and avoid the aforementioned risks.

I thank you very much in advance for your honor's attention.

Thank you,
Shantia Hassanshahi

Copy to: Engineer Namjoo, the Honorable Minister of Energy, for your information and ordering speedy action

1636

Address Redacted
[redacted] (805) 857-4246 - US Office
Address Redacted, CA 91361 [redacted] (310) 651-9680 - US FAX
[redacted] (213) 417-4086 – VOIP Phone

[2] This Persian calendar month refers to the period from July 23 to August 22, 2011 (Translator's note.)
[3] This Persian calendar month refers to the period from September 23 to October 22, 2011 (Translator's note.)

TRANSLATION NUMBER 185878. TRANSLATION FROM FARSI. Hasston letterhead to Haeri areva to company a **Page 2 of 2**

shantia34@gmail.com

TRANSLATION NUMBER 185878. TRANSLATION FROM FARSI. Hasston letterhead to Haeri areva to company a
Page 3 of 3

- On September 5, 2011, the Chief Executive of the intermediary Iranian company, Permayon, wrote a letter to the Iranian Minister of Energy expressing its version of events regarding the procurement of protection relays from COMPANY A. The writer stated Permayon divided its purchases into several phases when it placed orders for COMPANY A goods because it believed that low dollar amounts would not be noticed or scrutinized as closely and, specifically, that the true Iranian end-users for the goods would not be discovered.

23. Also found on **HASSANSHAHI**'s laptop computer was a letter (translated from Farsi to English), dated September 27, 2011, signed by **HASSANSHAHI** as "CEO/Managing Director" on KIAN DAY letterhead, and addressed to Majid Namjoo, the Iranian Minister of Energy. In the letter, **HASSANSHAHI** introduced KIAN DAY to the Iranian Minister of Energy as "founded in partnership with domestic engineers and Iranian investors residing overseas in order to obtain Hi-Tech technology, and localization of present-day science for the purpose of manufacturing small electrical meters." **HASSANSHAHI** then stated: "With the support of the honorable government of the Islamic Republic of Iran, our engineering group hopes to take effective steps in serving our beloved country and the electrical power industry."

24. Documentation found on **HASSANSHAHI**'s computer revealed that on November 19, 2011, and December 13, 2011, documents were filed by HIMAFAN and Permayon, respectively, at the Ministry of Justice of the Islamic Republic of Iran. The document filed by HIMAFAN claimed Permayon breached its financial obligations by not making payments, specifically to **HASSANSHAHI**, for the manufacture of goods. Permayon responded to this claim by calling the allegations unfounded and stated it was in fact HIMAFAN who caused the loss of confidence of the party to the FARS Electric contract.

25. Also found on **HASSANSHAHI**'s laptop computer was a letter authored by "Reza Baba'i" and addressed to Dr. Ayoub Shaban that specifically referenced various past and future engineering projects in Iran, for which **HASSANSHAHI** and his U.S. and Iranian companies are supplying the goods. Among other things, Baba'i stated the following in sum and substance:

- "KIAN DAY Company (Baba'I – Shantia [**HASSANSHAHI**]) is working in the meter business, and that business was conducted by Hima [HIMAFAN] in Iran and with the support of Shantia [**HASSANSHAHI**] in America."

- "Not considering Shantia [**HASSANSHAHI**] in business affairs is also a lie. Shantia [**HASSANSHAHI**] knows every business with everyone we have in Iran and abroad regarding relays and meters. We are partners. To date, we have over $3 million dollars in projects, and all of them has come through Shantia [**HASSANSHAHI**].

26. Also found on **HASSANSHAHI**'s laptop computer was an e-mail string between **HASSANSHAHI** and "Mark Babaei" in October 2009, concerning their intended transshipment of goods from Iraq into Iran. According to the e-mail string, on at least two occasions in 2009, **HASSANSHAHI**, doing business as **HASSTON**, ordered and shipped protection relays from "COMPANY A" in Canada to Iraq for declared use in the "Kurdistan Power Project" located there. In reality, however, the final destination for these relays was Iran. Throughout the e-mail string, **HASSANSHAHI** and "Babaei" discussed the logistics involved in moving the goods shipped to Iraq to the Iranian border for ultimate transshipment to that country. From my training and experience, had **HASSANSHAHI** accurately declared that Iran was the ultimate consignee for the goods, he would have been prohibited from shipping the goods there due to current sanctions against Iran.

27. HSI-DC has also contacted the U.S. Department of Treasury's Office of Foreign Asset Control ("OFAC") to ascertain whether **HASSANSHAHI, HASSTON,** or KIAN DAY have ever applied for an export license, authorizing **HASSANSHAHI, HASSTON,** or KIAN DAY to export any goods to Iran. **HASSANSHAHI, HASSTON, and** KIAN DAY have never applied for or obtained a license from OFAC, which is located in the District of Columbia, to export any goods to Iran.

28. In sum, I submit that there is probable cause to conclude that from at least 2009 to the present **SHANTIA HASSANSHAHI, also known as SHANTIA HASSAN SHAHI, also known as SHAHI, also known as SHANTIA HAAS, also known as SEAN HAAS, and HASSTON, INC**, both being "U.S. persons," have conspired to export goods to Iran without first having obtained the required export license from OFAC, in violation of the IEEPA, 50 U.S.C § 1705, and the ITR, 31 C.F.R. §§ 560.203 and 560.204.

_____
Joshua J. Akronowitz, Special Agent
U.S. Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn before me this _____ day of January, 2013.

_____
UNITED STATES MAGISTRATE JUDGE

Exhibit 2

Exhibit 2

AFFIDAVIT OF JOSHUA J. AKRONOWITZ

I, Joshua J. Akronowitz, being first duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so employed since 2007. I have received formal training in the laws and regulations relating to the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C §§ 1701-1706, and the Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R. Part 560, and have conducted and participated in investigations of the above listed laws and regulations.

2. On August 16, 2011, HSI received an unsolicited email from a voluntary source saying he had been contacted by an Iranian known as "M. Sheikhi, on behalf of Radyab Bartar Company." In his email to the source, Sheikhi asked for assistance in procuring "protection relays" from a company he identified as Areva. The email contained a list of parts he was interested in purchasing. Sheikhi's email also contained his signature block, which included his email address, radyab.bartar@gmail.com, and Iranian phone number, 982144406457, and the address of the company in Tehran, Iran.

3. On August 24, 2011, I sent a research request for information on phone number 982144406457, which is an Iranian phone number that was included in Sheikhi's signature block in the email he sent to the source. The research request was sent to an HSI-accessible law enforcement database.

4. On August 24, 2011, I reviewed the research provided in response to my request, which revealed that the Iranian phone number had been in contact with a domestic phone number, 818-971-9512, on one occasion, that is, on July 4, 2011. At the time I reviewed the response, the "818" number was the only U.S. phone number that had been in contact with the Iranian phone number. Based on my professional experience, because I once worked in Los Angeles, California, I recognized that the "818" area code was assigned to the Los Angeles County area. My request did not yield any other information that was useful to my investigation.

5. On August 16, 2011, I contacted an employee, who worked for Areva's Nuclear Parts Center, which is located in Lynchburg, Virginia. He agreed to examine the parts list provided in Sheikhi's email. I sent the list of parts to him on August 31, 2011, so that he could explain to me what the protection relays were, and whether they are export controlled.

6. On August 31, 2011, the Nuclear Parts Center employee explained that the parts are affiliated with a portion of Areva then known as Areva Transmission and Distribution, which had been sold to another company then known as Alstom Schneider Electric. He explained that protection relays are complex electromechanical devices that are

incorporated into and designed to calculate operating conditions on electrical circuits. They are generally intended to trip circuit breakers when a problem is detected in the circuit, in order to prevent damage to, or malfunctioning of, an electrical circuit or power grid. He said that he did not know whether all protection relays can be exported from the U.S. without a license, but some do require an export license from the U.S. Department of Commerce.

7. Even if a license was not required to export the protection relays, it would have been a violation of IEEPA and ITSR for a citizen or lawful permanent resident of the United States to export protection relays to Iran without permission from the U.S. Department of Treasury, Office of Foreign Assets and Control.

8. On September 9, 2011, I submitted an Administrative Export Enforcement Control Subpoena to Google for subscriber information and a list of IP addresses used for email account radyab.bartar@gmail.com.

9. On September 9, 2011, I entered Sheikhi's information in a law enforcement database known as TECS, so that I would be notified whenever Sheikhi traveled to the United States.

10. On September 20, 2011, another HSI special agent and I travelled to Vienna, Austria, where we conducted an interview with the source who submitted Sheikhi's email to HSI.

11. On September 27, 2011, I re-faxed the September 9th administrative subpoena to Google per their request. On September 29, 2011, Google sent me the information requested in the subpoena, that is, the subscriber information for email account radyab.bartar@gmail.com, and a log of the IP addresses where that email account was logged in and used.

12. On September 27, 2011, I performed a Google internet search on the "818" phone number to find out which phone company was assigned to that phone number. That open source internet search showed that the phone number was assigned to Bandwidth.com Inc. I then prepared and served an Administrative Export Enforcement Control Subpoena on Bandwidth.com Inc. to obtain subscriber and toll information for that phone number.

13. On October 4, 2011, I received a response from Bandwidth.com Inc., which stated that Bandwidth was not the service provider for the "818" number. Bandwidth's response indicated that Google/Google Voice was the current provider.

14. On October 6, 2011, I prepared and served an Administrative Export Enforcement Subpoena on Google/Google Voice for subscriber and toll information for phone number 818-971-9512.

15. On October 18, 2011, Google responded to my subpoena request with subscriber information showing that the "818" number was registered to Shantia Hassanshahi, with a particular home address in Westlake Village, California. Google also provided call log information for the period of September 6, 2011 to October 6, 2011, which showed numerous phone calls between Hassanshahi's "818" number and one Iranian phone number. Google's response also identified Hassanshahi's email address as shantia34@gmail.com.

16. On October 18, 2011, I conducted research on Hassanshahi in TECS and discovered the following information:

a. In 2003, Hassanshahi was under investigation by HSI/Oxnard, CA for conspiracy to violate IEEPA. The name and address information for Hassanshahi provided in the Oxnard investigation matched the name and address information Google provided for him in their subpoena return on October 18, 2011. The investigation by the HSI/Oxnard office revealed that Hassanshahi and two other partners had established an American company that attempted to enter into a contract with a Chinese company to build a computer production facility in Iran. Hassanshahi's company filed a breach of contract law suit against the Chinese company in California state court. That lawsuit was dismissed, in part because the contract involved doing business in Iran, and therefore was unenforceable because it was against public policy. The Department of Justice declined to file criminal charges against Hassanshahi and his partners.

b. On October 14, 2007, Hassanshahi returned from Mexico to the U.S. at the San Ysidro, CA port of entry as a passenger in a motor vehicle. Border officials determined that there was reason to investigate the vehicle, and as a result, Hassanshahi was interviewed by U.S. Customs and Border Protection officers. He was thereafter released and admitted into the United States.

c. In 2005, Hassanshahi was questioned by U.S. Customs and Border Protection officers when he returned from Dubai with $15,000 cash, which he had declared.

d. Records showed that in 2006, Hassanshahi returned from Tehran, Iran with a traveling companion.

e. Records showed that since 2006, Hassanshahi traveled to Iran four times: twice in 2008, once in 2010 and once in 2011. In fact, on the date of my research, the most recent record showed that Hassanshahi was still outside of the United States.

17. Based on the information about Hassanshahi that I learned from TECS, as well as from the other sources described above, I had reason to believe that Hassanshahi may have been attempting to help Sheihki, or someone else, export protection relays to Iran in violation of U.S. laws. Accordingly, on November 29, 2011, I augmented the existing

TECS records regarding Hassanshahi by entering instructions that I should be alerted if and when he returned to the United States, and that he should be referred for secondary screening by U.S. Customs and Border Protection officers when he returned to the U.S.

18. On December 20, 2011, I prepared and served an ICE Administrative Export Enforcement Subpoena on Google/Google Voice for subscriber information and recent internet protocol logs for the shantia34@gmail.com address. On January 10, 2012, Google responded to the subpoena. That response showed that the email account had been accessed in Iran 24 times between December 8 and December 15, 2011.

19. On January 11, 2012, I received an alert that Hassanshahi would be returning to the U.S. on January 12, 2012. He was scheduled to arrive on a flight at the Los Angeles International Airport ("LAX"). I alerted various law enforcement officials in Los Angeles to arrange for Hassanshahi's reception when he arrived. I could not participate in Hassanshahi's reception because I would be stationed at my office in Sterling, Virginia, when he was scheduled to arrive.

20. Law enforcement officials involved in Hassanshahi's secondary screening reported to me that on January 12, 2012, Hassanshahi arrived at LAX and presented himself for admission into the U.S. as an American citizen. He was then referred for a secondary screening with Homeland Security officers, and during that screening they detained his personal laptop computer and other electronic accessories. The laptop computer and accessories were mailed to me in Sterling, Virginia, for a forensic evaluation.

21. I received Hassanshahi's laptop computer and accessories on January 17, 2012, and they were submitted for forensic evaluation on the same day. A number of documents, including many that had to be translated from Farsi into English, were recovered from Hassanshahi's laptop. I mailed Hassanshahi's laptop and accessories to him on February 7, 2012.

I SWEAR OR AFFIRM THAT THE REPRESENTATIONS MADE ABOVE ARE TRUE AND CORRECT TO THE BEST OF MY INFORMATION, KNOWLEDGE, AND BELIEF.

Joshua J. Akronowitz, Special Agent
U.S. Department of Homeland Security
Homeland Security Investigations

Dated: July 9th, 2014

Subscribed and sworn to before me
This 9th day of July 2014
Washington, DC 20001

David A. Foster
Notary Public District of Columbia
My Commission Expires: May 14, 2015

Exhibit 3

Exhibit 3

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	Criminal No.: 13-274 (RC)
v.	:	
SHANTIA HASSANSHAHI,	:	
Defendant.	:	

THE UNITED STATES' REPLY TO DEFENDANT'S RESPONSE TO THE UNITED STATES' FEBRUARY 25, 2015 MEMORANDUM

Defendant's April 13, 2015 response (Def's Resp.) to the government's February 25, 2015 memorandum (Gov't Mem.) fails to adequately address the essential legal flaws in defendant's attempt to revisit the Court's denial of his earlier motion to suppress evidence. Defendant's attempt is flawed because he lacks standing to challenge the legitimacy of a subpoena that was issued to a third party. Additionally, even if the subpoena was issued in excess of the Drug Enforcement Administration's (DEA) statutory authority, such a statutory claim would not support suppression. Finally, defendant's assertion that the government has conceded a Fourth Amendment violation is simply wrong.

I. Defendant Lacks Standing To Contest the Validity of a Subpoena Issued to a Third Party

As the government explained in its opening memorandum, it is black letter law that a criminal defendant lacks standing to challenge the statutory validity of a subpoena issued to a third party. *See* Gov't Mem. at 5-6 (citing, *inter alia*, *United States v. Miller*, 425 U.S. 435, 444 (1976), *United States v. Moffett*, 84 F.3d 1291, 1293-94 (10th Cir. 1996), and *United States v. Phibbs*, 999 F.2d 1053, 1076-78 (6th Cir. 1993)). Defendant's only response is that he has standing to assert a ***constitutional*** violation. Def's Resp. at 7-8. This is a non sequitur.

To the extent that a defendant asserts a violation of his own legal rights, he has standing to do so. Hassanshahi did so in his original suppression motion, in which he claimed a violation of his Fourth Amendment rights. *See* Doc. # 28. While defendant had standing to make this motion, it lacked merit, and it was denied. *See United States v. Hassanshahi*, __ F. Supp. 3d __, 2014 WL 6735479 (D.D.C. Dec. 1, 2014). He is now attempting to assert a different legal theory—one based not on his constitutional rights, but on an allegation that a subpoena issued by the DEA was not authorized by 21 U.S.C. § 876. He lacks standing to raise this latter argument because, unlike the Fourth Amendment, Section 876 does not provide any rights to defendant and a defendant may not raise the purported statutory rights of the third-party subpoena recipient. *See* Gov't Mem. at 5-6; *United States v. Salvucci*, 448 U.S. 83 (1980); *United States v. Kember*, 648 F.2d 1354, 1365 (D.C. Cir. 1980) ("[T]he Supreme Court has made clear in recent years that a defendant has no standing to object to the introduction of evidence illegally seized from a third party.").

Because defendant's Fourth Amendment argument has already been rejected and defendant lacks standing to bring the statutory argument he now asserts, defendant should not be permitted to renew his motion to suppress.

II. There Is No Suppression Remedy for Use of an Administrative Subpoena in Violation of Statutory Authority

The government's opening memorandum explains in detail that there is no suppression remedy for a statutory violation unless the statute is itself a prophylactic protection of an individual constitutional right. *See* Gov't Mem. at 6-9.[1] Defendant attempts to elide this by

[1] The government's memorandum cited numerous Supreme Court and lower court holdings supporting this point of law. That memorandum also cited one Ninth Circuit case, *United States v. Dreyer*, 767 F.3d 826 (9th Cir. 2014), that appeared to be in tension with the rest of the caselaw. Since the filing of the government's memorandum, the Ninth Circuit has vacated the panel opinion in *Dreyer* and set the case for rehearing en banc. *See United States v. Dreyer*, __ F.3d __, 2015 WL 1344553 (Mar. 25, 2015).

reiterating his earlier claim of a Fourth Amendment violation. *See* Def's Resp. at 7. But his earlier claim was rejected on the ground that the evidence at issue is not the "fruit" of any purported Fourth Amendment violation. Defendant's new statutory claim can add nothing to this earlier claim because the statutory provision at issue is not a protection of defendant's constitutional rights. Indeed, any limitations on the DEA's subpoena authority exist to protect subpoena recipients and not other individuals. *See* Gov't Mem. at 5-6. The statute in this case is thus unlike the ones in cases in which a statutory violation has given rise to a suppression remedy,[2] and quite similar to the ones in the many cases in which courts have found no suppression remedy.[3]

III. The Government Has Not Conceded a Fourth Amendment Violation

Defendant's repeated allegations that the government has conceded a Fourth Amendment violation are false. As the Court is aware, HSI was initially alerted to defendant by a database search that provided a telephone call detail record indicating telephone communication between defendant and an Iranian believed to be attempting to import technologically sophisticated items in violation of U.S. sanctions law. In his initial motion to suppress, defendant contended that the database at issue "appears to [be] the [National Security Agency's] Bulk Telephony Metadata Program or some equivalent bulk telephone data collection program," or "[a]lternatively the

---

[2] *See* Gov't Mem. at 7-8 (discussing *McNabb v. United States*, 318 U.S. 332 (1943), and *Mallory v. United States*, 354 U.S. 449 (1957), which involved prophylactic protections of Fifth Amendment rights, and *Miller v. United States*, 357 U.S. 301 (1958), which involved a prophylactic protection of Fourth Amendment rights).

[3] *See* Gov't Mem. at 8-9 (discussing *United States v. Bourdet*, 477 F. Supp. 2d 164 (D.D.C. 2007); *see also United States v. Forrester*, 512 F.3d 500, 512-23 (9th Cir. 2008) (no suppression for violation of pen register statute); *United States v. Ani*, 138 F.3d 390, 392-93 (9th Cir. 1998) (no suppression for violation of regulation governing opening of international mail); *United States v. Mason*, 52 F.3d 1286, 1289 n.5 (4th Cir. 1995) (no suppression for search by customs agent in excess of statutory authority); *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995) (no suppression for violation of pen register statute); *United States v. Thompson*, 936 F.2d 1249, 1249-50 (11th Cir. 1991) (same).

government utilized some other historic, comprehensive database of calls . . . [which] 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." Doc. # 28, at 8. Defendant contended that this database violated his Fourth Amendment rights. *See id.* at 15-25. In making this assertion, defendant relied exclusively on Judge Leon's opinion in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *appeal pending*, No. 14-5004 (D.C. Cir.), in which Judge Leon found that the plaintiffs in that case were likely to prevail on their claim that the NSA's telephony metadata program violates the Fourth Amendment, *see id.* at 29. Defendant's brief contains numerous block quotations from *Klayman*, while citing no other legal authority for his contention that the database at issue was unconstitutional. *See* Doc. # 28, at 15-25.

In its opposition, the government argued that "there is no basis for allowing Hassanshahi to delve into the operation details of [the database at issue] because, even assuming that the query that returned a phone number associated with him was for some reason unlawful, there would be no basis for suppressing the evidence uncovered by the border search because the border search was sufficiently attenuated from the [database] query such that it is not the 'fruit' of that allegedly 'poisonous tree.'" Doc. # 37, at 5-6. Thus, the government argued, it was not necessary for the Court to analyze the database at issue or to assess the correctness of Judge Leon's opinion in *Klayman*, which was (and remains) on appeal before the D.C. Circuit. Nevertheless, the government made clear its position that the type of database defendant had posited, *i.e.*, a database of telephony metadata collected from telephone companies in bulk, would not violate the Fourth Amendment because "call records do not give rise to constitutional protection." *Id.* at 12 (citing, *inter alia*, *Smith v. Maryland*, 442 U.S. 735, 742-44 (1979), *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000), and *Reporters Comm. for*

Freedom of the Press v. AT&T, 593 F.2d 1030, 1042-46 (D.C. Cir. 1978)). The government further asserted that Judge Leon's analysis in *Klayman* was "'unpersuasive,'" *id.* at 13 (quoting *In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things*, Dkt. No. BR14-01, at 9 (For. Intel. Surv. Ct. Mar. 20, 2014) (Collyer, J.)), and noted that numerous other courts had rejected this analysis, *see id.* at 13 n.5. The government has also argued to the D.C. Circuit that Judge Leon's opinion is incorrect and that his decision should be reversed. *See Klayman v. Obama*, No. 14-5004 (D.C. Cir.).

In rejecting defendant's motion to suppress, this Court agreed with the government's attenuation analysis. Thus, the Court found it unnecessary to determine whether *Klayman* was correctly decided, and it observed that "federal courts generally have approved of the NSA [telephony metadata] program, with the exception of Judge Leon's opinion in *Klayman*, which itself is on appeal before the D.C. Circuit." *Hassanshahi*, 2014 WL 6735479, at *8.

If, as the government has consistently maintained, *Klayman* was wrongly decided, then Hassanshahi's Fourth Amendment claim is entirely lacking in legal foundation. Even if *Klayman* were correct, however, it would not establish that the DEA's now-defunct database violated the Fourth Amendment. Unlike the NSA's database, and contrary to defendant's allegations, the DEA database component at issue contained call detail records relating only to certain international calls, namely calls from the United States to certain designated foreign countries, including Iran. Doc. # 49-1, ¶ 4. And, even if, contra *Smith v. Maryland*, an individual could claim a Fourth Amendment protected interest in the call records of domestic telephone calls, it dubious that he could claim such an interest in the call records of *international* telephone calls. *See United States v. Ramsey*, 431 U.S. 606, 607-08 (1977) (holding that the government may conduct suspicionless searches of the contents of international letters); *id.* at

623 n.17 ("There are limited justifiable expectations of privacy for incoming material crossing United States borders.").

Given this Court's correct attenuation analysis in its December 1, 2014 opinion, it is unnecessary for this Court to opine as to the constitutionality of DEA's now-defunct database component or the correctness of *Klayman*. But to the extent Hassanshahi claims that the government has conceded either of these points, he is mistaken.

Conclusion

Defendant's assertion of statutory violation by DEA provides no basis for suppressing the evidence obtained from defendant's laptop computer.

April 29, 2015

Respectfully submitted,

VINCENT H. COHEN, Jr.
Acting United States Attorney

FREDERICK YETTE, D.C. Bar 385391
Assistant United States Attorney
National Security Section
555 4th Street, N.W.
Washington, D.C. 20530

/s/ Jeffrey M. Smith
JEFFREY M. SMITH, D.C. Bar 467936
Appellate Unit
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

Exhibit 4

Exhibit 4

U.S. secretly tracked billions of calls for decades

Brad Heath, USA TODAY *10:36 a.m. EDT April 8, 2015*

A USA TODAY investigation revealed that a secret program collecting phone call data for international calls started in 1992. USA TODAY

(Photo: Photo: Mike Christy, AP)

WASHINGTON — The U.S. government started keeping secret records of Americans' international telephone calls nearly a decade before the Sept. 11 terrorist attacks, harvesting billions of calls in a program that provided a blueprint for the far broader National Security Agency surveillance that followed.

For more than two decades, the Justice Department and the Drug Enforcement Administration amassed logs of virtually all telephone calls from the USA to as many as 116 countries linked to drug trafficking, current and former officials involved with the operation said. The targeted countries changed over time but included Canada, Mexico and most of Central and South America.

Federal investigators used the call records to track drug cartels' distribution networks in the USA, allowing agents to detect previously unknown trafficking rings and money handlers. They also used the records to help rule out foreign ties to the bombing in 1995 of a federal building in Oklahoma City and to identify U.S. suspects in a wide range of other investigations.

The Justice Department revealed in January (/story/news/nation/2015/01/16/phone-database-justice/21868063/) that the DEA had collected data (https://www.documentcloud.org/documents/1719876-database.html#document/p2/a212333) about calls to "designated foreign countries." But the history and vast scale of that operation have not been disclosed until now.

The now-discontinued operation, carried out by the DEA's intelligence arm, was the government's first known effort to gather data on Americans in bulk, sweeping up records of telephone calls made by millions of U.S. citizens regardless of whether they were suspected of a crime. It was a model for the massive phone surveillance system the NSA launched to identify terrorists after the Sept. 11 attacks. That dragnet drew sharp criticism that the government had intruded too deeply into Americans' privacy after former NSA contractor Edward Snowden leaked it to the news media two years ago.

More than a dozen current and former law enforcement and intelligence officials described the details of the Justice Department operation to USA TODAY. Most did so on the condition of anonymity because they were not authorized to publicly discuss the intelligence program, part of which remains classified.

The DEA program did not intercept the content of Americans' calls, but the records — which numbers were dialed and when — allowed agents to map suspects' communications and link them to troves of other police and intelligence data. At first, the drug agency did so with help from military computers and intelligence analysts.

That data collection was "one of the most important and effective Federal drug law enforcement initiatives," the Justice Department said in a 1998 letter to Sprint asking the telecom giant to turn over its call records. The previously undisclosed letter was signed by the head of the department's Narcotics and Dangerous Drugs Section, Mary Lee Warren, who wrote that the operation had "been approved at the highest levels of Federal law enforcement authority," including then-Attorney General Janet Reno and her deputy, Eric Holder.

Attorney General Janet Reno, accompanied by Deputy Attorney General Eric Holder, meets reporters at the Justice Department in Washington Aug. 4, 1998. Both approved the DEA phone data collection, according to a Justice Department letter sent to Sprint executives that year. *(Photo: KHUE BUI, AP)*

The data collection began in 1992 during the administration of President George H.W. Bush, nine years before his son, President George W. Bush, authorized the NSA to gather its own logs of Americans' phone calls in 2001. It was approved by top Justice Department officials in four presidential administrations and detailed in occasional briefings to members of Congress but otherwise had little independent oversight, according to officials involved with running it.

The DEA used its data collection extensively and in ways that the NSA is now prohibited from doing. Agents gathered the records without court approval, searched them more often in a day than the spy agency does in a year and automatically linked the numbers the agency gathered to large electronic collections of investigative reports, domestic call records accumulated by its agents and intelligence data from overseas.

The result was "a treasure trove of very important information on trafficking," former DEA administrator Thomas Constantine said in an interview.

The extent of that surveillance alarmed privacy advocates, who questioned its legality. "This was aimed squarely at Americans," said Mark Rumold, an attorney with the Electronic Frontier Foundation. "That's very significant from a constitutional perspective."

Holder halted the data collection in September 2013 amid the fallout from Snowden's revelations about other surveillance programs. In its place, current and former officials said the drug agency sends telecom companies daily subpoenas for international calling records involving only phone numbers that agents suspect are linked to the drug trade or other crimes — sometimes a thousand or more numbers a day.

Tuesday, Justice Department spokesman Patrick Rodenbush said the DEA "is no longer collecting bulk telephony metadata from U.S. service providers." A DEA spokesman declined to comment.

HARVESTING DATA TO BATTLE CARTELS

The DEA began assembling a data-gathering program in the 1980s as the government searched for new ways to battle Colombian drug cartels. Neither informants nor undercover agents had been enough to crack the cartels' infrastructure. So the agency's intelligence arm turned its attention to the groups' communication networks.

Calling records – often called "toll records" – offered one way to do that. Toll records are comparable to what appears on a phone bill – the numbers a person dialed, the date and time of the call, its duration and how it was paid for. By then, DEA agents had decades of experience gathering toll records of people they suspected were linked to drug trafficking, albeit one person at a time. In the late 1980s and early 1990s, officials said the agency had little way to make sense of the data their agents accumulated and almost no ability to use them to ferret out new cartel connections. Some agents used legal pads.

"We were drowning in toll records," a former intelligence official said.

The DEA asked the Pentagon for help. The military responded with a pair of supercomputers and intelligence analysts who had experience tracking the communication patterns of Soviet military units. "What they discovered was that the incident of a communication was perhaps as important as the content of a communication," a former Justice Department official said.

The military installed the supercomputers on the fifth floor of the DEA's headquarters, across from a shopping mall in Arlington, Va.

The system they built ultimately allowed the drug agency to stitch together huge collections of data to map trafficking and money laundering networks both overseas and within the USA. It allowed agents to link the call records its agents gathered domestically with calling data the DEA and intelligence agencies had acquired outside the USA. (In some cases, officials said the DEA paid employees of foreign telecom firms for copies of call logs and subscriber lists.) And it eventually allowed agents to cross-reference all of that against investigative reports from the DEA, FBI and Customs Service.

Thomas Constantine, the head of the U.S. Drug Enforcement Agency, boards the US Coast Guard cutter Gallatin in San Juan, Puerto Rico, on April 3, 1997. *(Photo: John McConnico, AP)*

The result "produced major international investigations that allowed us to take some big people," Constantine said, though he said he could not identify particular cases.

In 1989, President George H.W. Bush proposed in his first prime-time address using "sophisticated intelligence-gathering and Defense Department technology" to disrupt drug trafficking. Three years later, when violent crime rates were at record highs, the drug agency intensified its intelligence push, launching a "kingpin strategy" to attack drug cartels by going after their finances, leadership and communication.

THE START OF BULK COLLECTION

In 1992, in the last months of Bush's administration, Attorney General William Barr and his chief criminal prosecutor, Robert Mueller, gave the DEA permission to collect a much larger set of phone data to feed into that intelligence operation.

Instead of simply asking phone companies for records about calls made by people suspected of drug crimes, the Justice Department began ordering telephone companies to turn over lists of all phone calls from the USA to countries where the government determined drug traffickers operated, current and former officials said.

Barr and Mueller declined to comment, as did Barr's deputy, George Terwilliger III, though Terwilliger said, "It has been apparent for a long time in both the law enforcement and intelligence worlds that there is a tremendous value and need to collect certain metadata to support legitimate investigations."

The data collection was known within the agency as USTO (a play on the fact that it tracked calls from the U.S. to other countries).

The DEA obtained those records using administrative subpoenas that allow the agency to collect records "relevant or material to" federal drug investigations. Officials acknowledged it was an expansive interpretation of that authority but one that was not likely to be challenged because unlike search warrants, DEA subpoenas do not require a judge's approval. "We knew we were stretching the definition," a former official involved in the process said.

Officials said a few telephone companies were reluctant to provide so much information, but none challenged the subpoenas in court. Those that hesitated received letters from the Justice Department urging them to comply.

Former deputy assistant attorney general Mary Lee Warren speaks with a Colombian prosecutor in 2007. Warren wrote a letter in 1998, asking Sprint to turn over telephone records. *(Photo: MAURICIO DUENAS, AFP/Getty Images)*

After Sprint executives expressed reservations in 1998, for example, Warren, the head of the department's drug section, responded with a letter telling the company that "the initiative has been determined to be legally appropriate" and that turning over the call data was "appropriate and required by law." The letter said the data would be used by authorities "to focus scarce investigative resources by means of sophisticated pattern and link analysis."

The letter did not name other telecom firms providing records to the DEA but did tell executives that "the arrangement with Sprint being sought by the DEA is by no means unique to Sprint" and that "major service providers have been eager to support and assist law enforcement within appropriate bounds." Former officials said the operation included records from AT&T and other telecom companies.

A spokesman for AT&T declined to comment. Sprint spokeswoman Stephanie Vinge Walsh said only that "we do comply with all state and federal laws regarding law enforcement subpoenas."

Agents said that when the data collection began, they sought to limit its use mainly to drug investigations and turned away requests for access from the FBI and the NSA. They allowed searches of the data in terrorism cases, including the bombing of a federal building in Oklahoma City that killed 168 people in 1995, helping to rule out theories linking the attack to foreign terrorists. They allowed even broader use after Sept. 11, 2001. The DEA's public disclosure of its program in January (https://www.documentcloud.org/documents/1719876-database.html) came in the case of a man charged with violating U.S. export restrictions by trying to send electrical equipment to Iran.

At first, officials said the DEA gathered records only of calls to a handful of countries, focusing on Colombian drug cartels and their supply lines. Its reach grew quickly, and by the late 1990s, the DEA was logging "a massive number of calls," said a former intelligence official who supervised the program.

Former officials said they could not recall the complete list of countries included in USTO, and the coverage changed over time. The Justice Department and DEA added countries to the list if officials could establish that they were home to outfits that produced or trafficked drugs or were involved in money laundering or other drug-related crimes.

The Justice Department warned when it disclosed the program in January (https://www.documentcloud.org/documents/1700104-d-d-c-13-cr-00274-dckt-000049-000-filed-2015-01-15.html#document/p3/a211046) that the list of countries should remain secret "to protect against any disruption to prospective law enforcement cooperation."

At its peak, the operation gathered data on calls to 116 countries, an official involved in reviewing the list said. Two other officials said they did not recall the precise number of countries, but it was more than 100. That gave the collection a considerable sweep; the U.S. government recognizes a total of 195 countries (http://www.state.gov/s/inr/rls/4250.htm).

At one time or another, officials said, the data collection covered most of the countries in Central and South America and the Caribbean, as well as others in western Africa, Europe and Asia. It included Afghanistan, Pakistan, Iran, Italy, Mexico and Canada.

The DEA often — though not always — notified foreign governments it was collecting call records, in part to make sure its agents would not be expelled if the program was discovered. In some cases, the DEA provided some of that information to foreign law enforcement agencies to help them build their own investigations, officials said.

The DEA did not have a real-time connection to phone companies' data; instead, the companies regularly provided copies of their call logs, first on computer disks and later over a private network. Agents who used the system said the numbers they saw were seldom more than a few days old.

The database did not include callers' names or other identifying data. Officials said agents often were able to identify individuals associated with telephone numbers flagged by the analysis, either by cross-referencing them against other databases or by sending follow-up requests to the phone companies.

To keep the program secret, the DEA sought not to use the information as evidence in criminal prosecutions or in its justification for warrants or other searches. Instead, its Special Operations Division passed the data to field agents as tips to help them find new targets or focus existing investigations, a process approved by Justice Department lawyers. Many of those tips were classified because the DEA phone searches drew on other intelligence data.

That practice sparked a furor when the Reuters news agency reported in 2013 (http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805) that the DEA trained agents to conceal the sources of those tips from judges and defense lawyers. Reuters said the tips were based on wiretaps, foreign intelligence and a DEA database of telephone calls gathered through routine subpoenas and search warrants.

As a result, "the government short-circuited any debate about the legality and wisdom of putting the call records of millions of innocent people in the hands of the DEA," American Civil Liberties Union lawyer Patrick Toomey said.

Listen to Brad Heath detail his investigation into decades of bulk data collection in the audio player below:

A BLUEPRINT FOR BROADER SURVEILLANCE

The NSA began collecting its own data on Americans' phone calls within months of Sept. 11, 2001, as a way to identify potential terrorists within the USA. At first, it did so without court approval. In 2006, after *The New York Times* (http://www.nytimes.com/2005/12/16/politics/16program.html?hp&_r=0) and USA TODAY (http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm) began reporting on the surveillance program, President George W. Bush's administration brought it under the Foreign Intelligence Surveillance Act, which allows the government to use secret court orders to get access to records relevant to national security investigations. Unlike the DEA, the NSA also gathered logs of calls within the USA.

The similarities between the NSA program and the DEA operation established a decade earlier are striking – too much so to have been a coincidence, people familiar with the programs said. Former NSA general counsel Stewart Baker said, "It's very hard to see (the DEA operation) as anything other than the precursor" to the NSA's terrorist surveillance.

Both operations relied on an expansive interpretation of the word "relevant," for example — one that allowed the government to collect vast amounts of information on the premise that some tiny fraction of it would be useful to investigators. Both used similar internal safeguards, requiring analysts to certify that they had "reasonable articulable suspicion" – a comparatively low legal threshold – that a phone number was linked to a drug or intelligence case before they could query the records.

"The foundation of the NSA program was a mirror image of what we were doing," said a former Justice Department official who helped oversee the surveillance. That official said he and others briefed NSA lawyers several times on the particulars of their surveillance program. Two former DEA officials also said the NSA had been briefed on the operation. The NSA declined to comment.

There were also significant differences.

For one thing, DEA analysts queried their data collection far more often. The NSA said analysts searched its telephone database only about 300 times in 2012; DEA analysts routinely performed that many searches in a day, former officials said. Beyond that, NSA analysts must have approval from a judge on the Foreign Intelligence Surveillance Court each time they want to search their own collection of phone metadata, and they do not automatically cross-reference it (https://www.documentcloud.org/documents/1694968-nsa-declaration.html#document/p8/a210174) with other intelligence files.

Sen. Patrick Leahy, D-Vt., then the chairman of the Senate Judiciary Committee, complained last year to Holder that the DEA had been gathering phone data "in bulk" without judicial oversight. Officials said the DEA's database was disclosed to judges only occasionally, in classified hearings.

For two decades, it was never reviewed by the Justice Department's own inspector general, which told Congress it is now looking into (https://www.documentcloud.org/documents/1698394-2015-02-23.html) the DEA's bulk data collections.

A SMALLER SCALE COLLECTION

Holder pulled the plug on the phone data collection in September 2013.

That summer, Snowden leaked a remarkable series of classified documents detailing some of the government's most prized surveillance secrets, including the NSA's logging of domestic phone calls and Internet traffic. Reuters (http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805) and *The New York Times* (http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html?_r=0) raised questions about the drug agency's own access to phone records.

Officials said the Justice Department told the DEA that it had determined it could not continue both surveillance programs, particularly because part of its justification for sweeping NSA surveillance was that it served national security interests, not ordinary policing. Eight months after USTO was halted, for example, department lawyers defended the spy agency's phone dragnet in court partly on the grounds that it "serves special governmental needs above and beyond normal law enforcement."

Three months after USTO was shut down, a review panel commissioned by President Obama urged Congress to bar the NSA from gathering telephone data on Americans in bulk. Not long after that, Obama instructed the NSA to get permission from the surveillance court before querying its phone data collection, a step the drug agency never was required to take.

The DEA stopped searching USTO in September 2013. Not long after that, it purged the database.

U.S. Attorney General Eric Holder speaks on criminal justice and sentencing at the National Press Club on Feb. 17 in Washington. *(Photo: MANDEL NGAN, AFP/Getty Images)*

"It was made abundantly clear that they couldn't defend both programs," a former Justice Department official said. Others said Holder's message was more direct. "He said he didn't think we should have that information," a former DEA official said.

By then, agents said USTO was suffering from diminishing returns. More criminals — especially the sophisticated cartel operatives the agency targeted — were communicating on Internet messaging systems that are harder for law enforcement to track.

Still, the shutdown took a toll, officials said. "It has had a major impact on investigations," one former DEA official said.

The DEA asked the Justice Department to restart the surveillance program in December 2013. It withdrew that request when agents came up with a new solution. Every day, the agency assembles a list of the telephone numbers its agents suspect may be tied to drug trafficking. Each day, it sends electronic subpoenas — sometimes listing more than a thousand numbers — to telephone companies seeking logs of international telephone calls linked to those numbers, two official familiar with the program said.

The data collection that results is more targeted but slower and more expensive. Agents said it takes a day or more to pull together communication profiles that used to take minutes.

The White House proposed a similar approach for the NSA's telephone surveillance program (https://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m), which is set to expire June 1. That approach would halt the NSA's bulk data collection but would give the spy agency the power to force companies to turn over records linked to particular telephone numbers, subject to a court order.

Follow investigative reporter Brad Heath on Twitter at @bradheath (http://twitter.com/bradheath).

The Justice Department began secretly collecting records of Americans' international phone calls in 1992.

Read or Share this story: http://usat.ly/1FyBMkt

TOP VIDEOS

/videos/news/2632390400001/4368171631001

Car hacking: should you worry? (/videos/news/2632390400001/43

01:51

Donald Trump wealth details released

(/videos/news/2632390400001/4368175161001

(/videos/news/2632390400001/4368175161001)

00:49

McDonald's may begin serving all-day breakfast

(/videos/news/2632390400001/4368144891001

(/videos/news/2632390400001/4368144891001)

00:44

Exhibit 5

Exhibit 5

The Intercept_

THE SURVEILLANCE ENGINE

How the NSA Built Its Own Secret Google

266

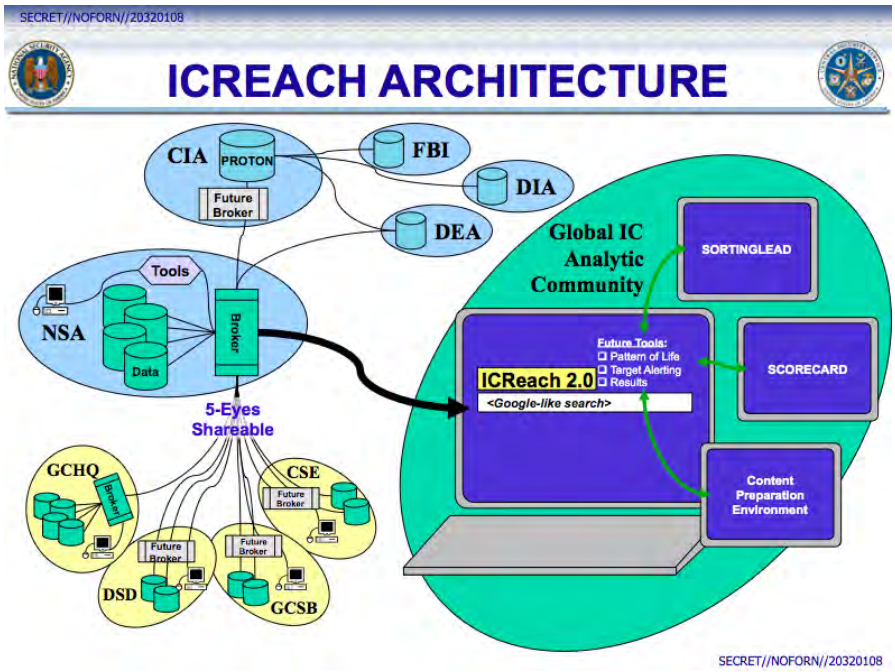
Ryan Gallagher
Aug. 25 2014, 10:09 a.m.

The National Security Agency is secretly providing data to nearly two dozen U.S. government agencies with a "Google-like" search engine built to share more than 850 billion records about phone calls, emails, cellphone locations, and internet chats, according to classified documents obtained by *The Intercept*.

The documents provide the first definitive evidence that the NSA has for years made massive amounts of surveillance data directly accessible to domestic law enforcement agencies. Planning documents for ICREACH, as the search engine is called, cite the Federal Bureau of Investigation and the Drug Enforcement Administration as key participants.

ICREACH contains information on the private communications of foreigners and, it appears, millions of records on American citizens who have not been accused of any wrongdoing. Details about its existence are contained in the archive of materials provided to *The Intercept* by NSA whistleblower Edward Snowden.

Earlier revelations sourced to the Snowden documents have exposed a multitude of NSA programs for collecting large volumes of communications. The NSA has acknowledged that it shares some of its collected data with domestic agencies like the FBI, but details about the method and scope of its sharing have remained shrouded in secrecy.



ICREACH has been accessible to more than 1,000 analysts at 23 U.S. government agencies that perform intelligence work, according to a 2010 memo. A planning document from 2007 lists the DEA, FBI, Central Intelligence Agency, and the Defense Intelligence Agency as core members. Information shared through ICREACH can be used to track people's movements, map out their networks of associates, help predict future actions, and potentially reveal religious affiliations or political beliefs.

The creation of ICREACH represented a landmark moment in the history of classified U.S. government surveillance, according to the NSA documents.

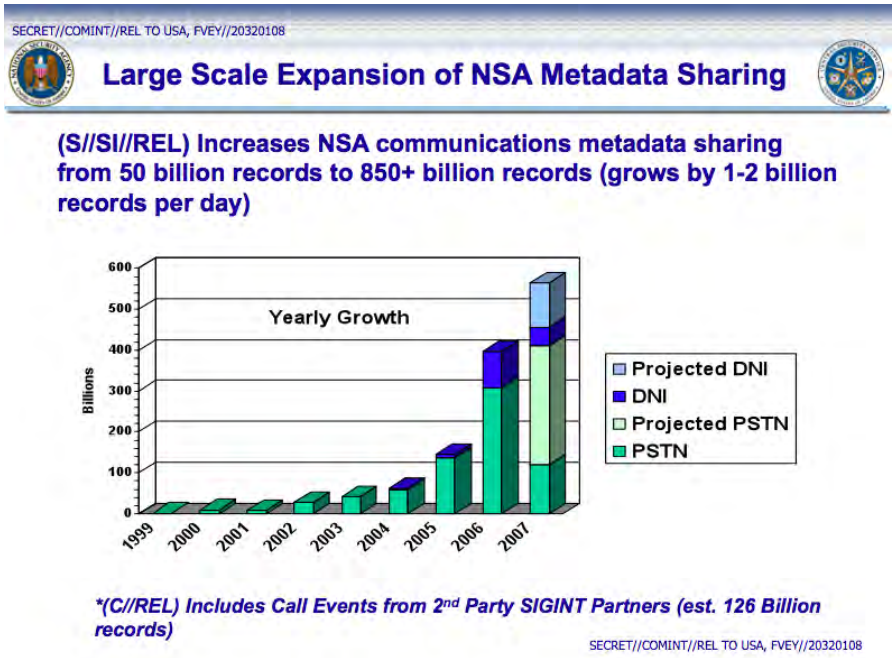
"The ICREACH team delivered the first-ever

wholesale sharing of communications metadata within the U.S. Intelligence Community," noted a top-secret memo dated December 2007. "This team began over two years ago with a basic concept compelled by the IC's increasing need for communications metadata and NSA's ability to collect, process and store vast amounts of communications metadata related to worldwide intelligence targets."

The search tool was designed to be the largest system for internally sharing secret surveillance records in the United States, capable of handling two to five billion new records every day, including more than 30 different kinds of metadata on emails, phone calls, faxes, internet chats, and text messages, as well as location information collected from cellphones. Metadata reveals information about a communication – such as the "to" and "from" parts of an email, and the time and date it was sent, or the phone numbers someone called and when they called – but not the content of the message or audio of the call.

ICREACH does not appear to have a direct relationship to the large NSA database, previously reported by *The Guardian*, that stores information on millions of ordinary Americans' phone calls under Section 215 of the Patriot Act.

Unlike the 215 database, which is accessible to a small number of NSA employees and can be searched only in terrorism-related investigations, ICREACH grants access to a vast pool of data that can be mined by analysts from across the intelligence community for "foreign intelligence" – a vague term that is far broader than counterterrorism.



Data available through ICREACH appears to be primarily derived from surveillance of foreigners' communications, and planning documents show that it draws on a variety of different sources of data maintained by the NSA. Though one 2010 internal paper clearly calls it "the ICREACH database," a U.S. official familiar with the system disputed that, telling *The*

Intercept that while "it enables the sharing of certain foreign intelligence metadata," ICREACH is "not a repository [and] does not store events or records." Instead, it appears to provide analysts with the ability to perform a one-stop search of information from a wide variety of separate databases.

In a statement to *The Intercept*, the Office of the Director of National Intelligence confirmed that the system shares data that is swept up by programs authorized under Executive Order 12333, a controversial Reagan-era presidential directive that underpins several NSA bulk surveillance operations that monitor communications overseas. The 12333 surveillance takes place with no court oversight and has received minimal Congressional scrutiny because it is targeted at foreign, not domestic, communication networks. But the broad scale of 12333 surveillance means that some Americans' communications get caught in the dragnet as they transit international cables or satellites – and documents contained in the Snowden archive indicate that ICREACH taps into some of that data.

Legal experts told *The Intercept* they were shocked to learn about the scale of the ICREACH system and are concerned that law enforcement

authorities might use it for domestic investigations that are not related to terrorism.

“To me, this is extremely troublesome,” said Elizabeth Goitein, co-director of the Liberty and National Security Program at the New York University School of Law’s Brennan Center for Justice. “The myth that metadata is just a bunch of numbers and is not as revealing as actual communications content was exploded long ago – this is a trove of incredibly sensitive information.”

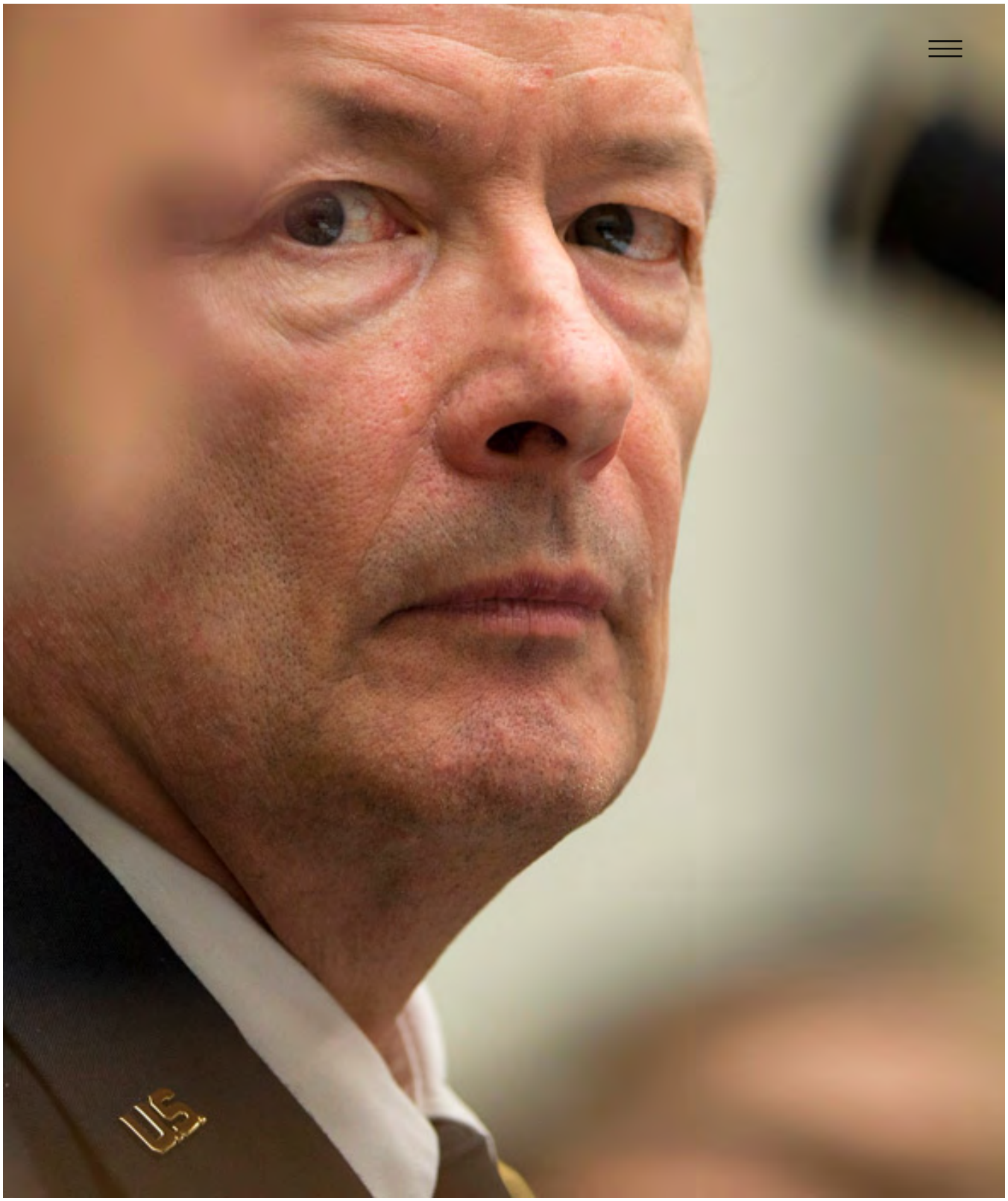
Brian Owsley, a federal magistrate judge between 2005 and 2013, said he was alarmed that traditional law enforcement agencies such as the FBI and the DEA were among those with access to the NSA’s surveillance troves.

“This is not something that I think the government should be doing,” said Owsley, an assistant professor of law at Indiana Tech Law School. “Perhaps if information is useful in a specific case, they can get judicial authority to provide it to another agency. But there shouldn’t be this buddy-buddy system back-and-forth.”

Jeffrey Anchukaitis, an ODNI spokesman, declined to comment on a series of questions

from *The Intercept* about the size and scope of ICREACH, but said that sharing information had become "a pillar of the post-9/11 intelligence community" as part of an effort to prevent valuable intelligence from being "stove-piped in any single office or agency."

Using ICREACH to query the surveillance data, "analysts can develop vital intelligence leads without requiring access to raw intelligence collected by other IC [Intelligence Community] agencies," Anchukaitis said. "In the case of NSA, access to raw signals intelligence is strictly limited to those with the training and authority to handle it appropriately. The highest priority of the intelligence community is to work within the constraints of law to collect, analyze and understand information related to potential threats to our national security."

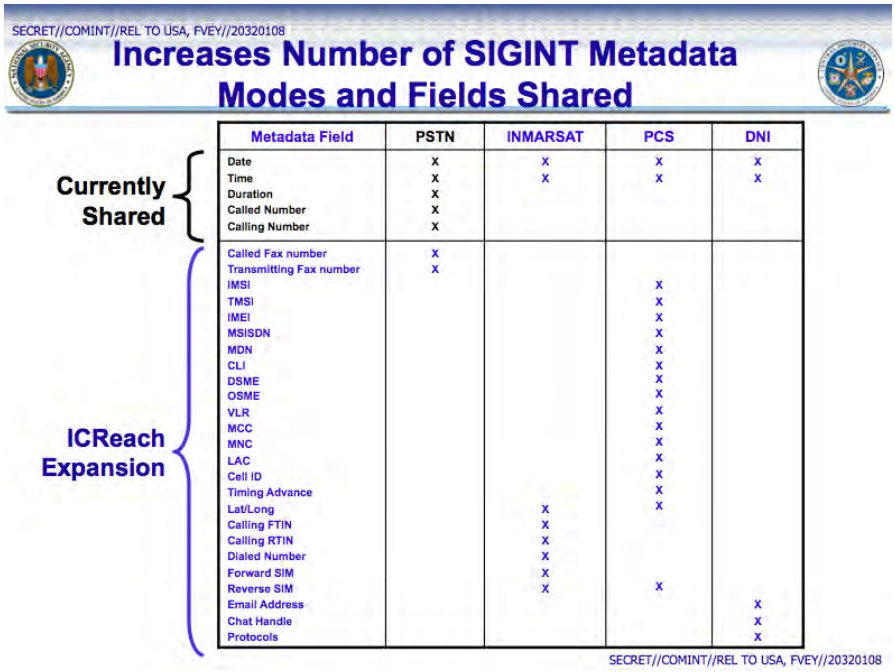


One-Stop Shopping

The mastermind behind ICREACH was recently retired NSA director Gen. Keith Alexander, who outlined his vision for the system in a classified 2006 letter to the then-Director of National Intelligence John Negroponte. The search tool, Alexander wrote, would "allow unprecedented volumes of communications metadata to be shared and analyzed," opening up a "vast, rich source of information" for other agencies to exploit. By late 2007 the NSA reported to its employees that the system had gone live as a pilot program.

The NSA described ICREACH as a "one-stop shopping tool" for analyzing communications. The system would enable at least a 12-fold increase in the volume of metadata being shared between intelligence community agencies, the documents stated. Using ICREACH, the NSA planned to boost the amount of communications "events" it shared with other U.S. government agencies from 50 billion to more than 850 billion, bolstering an older top-secret data sharing system named CRISSCROSS/PROTON, which was launched in the 1990s and managed by the CIA.

To allow government agents to sift through the masses of records on ICREACH, engineers designed a simple "Google-like" search interface. This enabled analysts to run searches against particular "selectors" associated with a person of interest – such as an email address or phone number – and receive a page of results displaying, for instance, a list of phone calls made and received by a suspect over a month-long period. The documents suggest these results can be used reveal the "social network" of the person of interest – in other words, those that they communicate with, such as friends, family, and other associates.



The purpose of ICREACH, projected initially to cost between $2.5 million and $4.5 million per

year, was to allow government agents to comb through the NSA's metadata troves to identify new leads for investigations, to predict potential future threats against the U.S., and to keep tabs on what the NSA calls "worldwide intelligence targets."

However, the documents make clear that it is not only data about foreigners' communications that are available on the system. Alexander's memo states that "many millions of…minimized communications metadata records" would be available through ICREACH, a reference to the process of "minimization," whereby identifying information – such as part of a phone number or email address – is removed so it is not visible to the analyst. NSA documents define minimization as "specific procedures to minimize the acquisition and retention [of] information concerning unconsenting U.S. persons" – making it a near certainty that ICREACH gives analysts access to millions of records about Americans. The "minimized" information can still be retained under NSA rules for up to five years and "unmasked" at any point during that period if it is ever deemed necessary for an investigation.

The Brennan Center's Goitein said it appeared that with ICREACH, the government "drove a

truck" through loopholes that allowed it to circumvent restrictions on retaining data about Americans. This raises a variety of legal and constitutional issues, according to Goitein, particularly if the data can be easily searched on a large scale by agencies like the FBI and DEA for their domestic investigations.

"The idea with minimization is that the government is basically supposed to pretend this information doesn't exist, unless it falls under certain narrow categories," Goitein said. "But functionally speaking, what we're seeing here is that minimization means, 'we'll hold on to the data as long as we want to, and if we see anything that interests us then we can use it.'"

A key question, according to several experts consulted by *The Intercept*, is whether the FBI, DEA or other domestic agencies have used their access to ICREACH to secretly trigger investigations of Americans through a controversial process known as "parallel construction."

Parallel construction involves law enforcement agents using information gleaned from covert surveillance, but later covering up their use of that data by creating a new evidence trail that excludes it. This hides the true origin of the

investigation from defense lawyers and, on occasion, prosecutors and judges – which means the legality of the evidence that triggered the investigation cannot be challenged in court.

In practice, this could mean that a DEA agent identifies an individual he believes is involved in drug trafficking in the United States on the basis of information stored on ICREACH. The agent begins an investigation but pretends, in his records of the investigation, that the original tip did not come from the secret trove. Last year, Reuters first reported details of parallel construction based on NSA data, linking the practice to a unit known as the Special Operations Division, which Reuters said distributes tips from NSA intercepts and a DEA database known as DICE.

Tampa attorney James Felman, chair of the American Bar Association's criminal justice section, told *The Intercept* that parallel construction is a "tremendously problematic" tactic because law enforcement agencies "must be honest with courts about where they are getting their information." The ICREACH revelations, he said, "raise the question of whether parallel construction is present in more cases than we had thought. And if that's true, it is deeply disturbing and disappointing."

Anchukaitis, the ODNI spokesman, declined to say whether ICREACH has been used to aid domestic investigations, and he would not name all of the agencies with access to the data. "Access to information-sharing tools is restricted to users conducting foreign intelligence analysis who have the appropriate training to handle the data," he said.

CIA headquarters in Langley, Virginia, 2001.

Project CRISSCROSS

The roots of ICREACH can be traced back more than two decades.

In the early 1990s, the CIA and the DEA embarked on a secret initiative called Project

CRISSCROSS. The agencies built a database system to analyze phone billing records and phone directories, in order to identify links between intelligence targets and other persons of interest. At first, CRISSCROSS was used in Latin America and was "extremely successful" at identifying narcotics-related suspects. It stored only five kinds of metadata on phone calls: date, time, duration, called number, and calling number, according to an NSA memo.

The program rapidly grew in size and scope. By 1999, the NSA, the Defense Intelligence Agency, and the FBI had gained access to CRISSCROSS and were contributing information to it. As CRISSCROSS continued to expand, it was supplemented with a system called PROTON that enabled analysts to store and examine additional types of data. These included unique codes used to identify individual cellphones, location data, text messages, passport and flight records, visa application information, as well as excerpts culled from CIA intelligence reports.

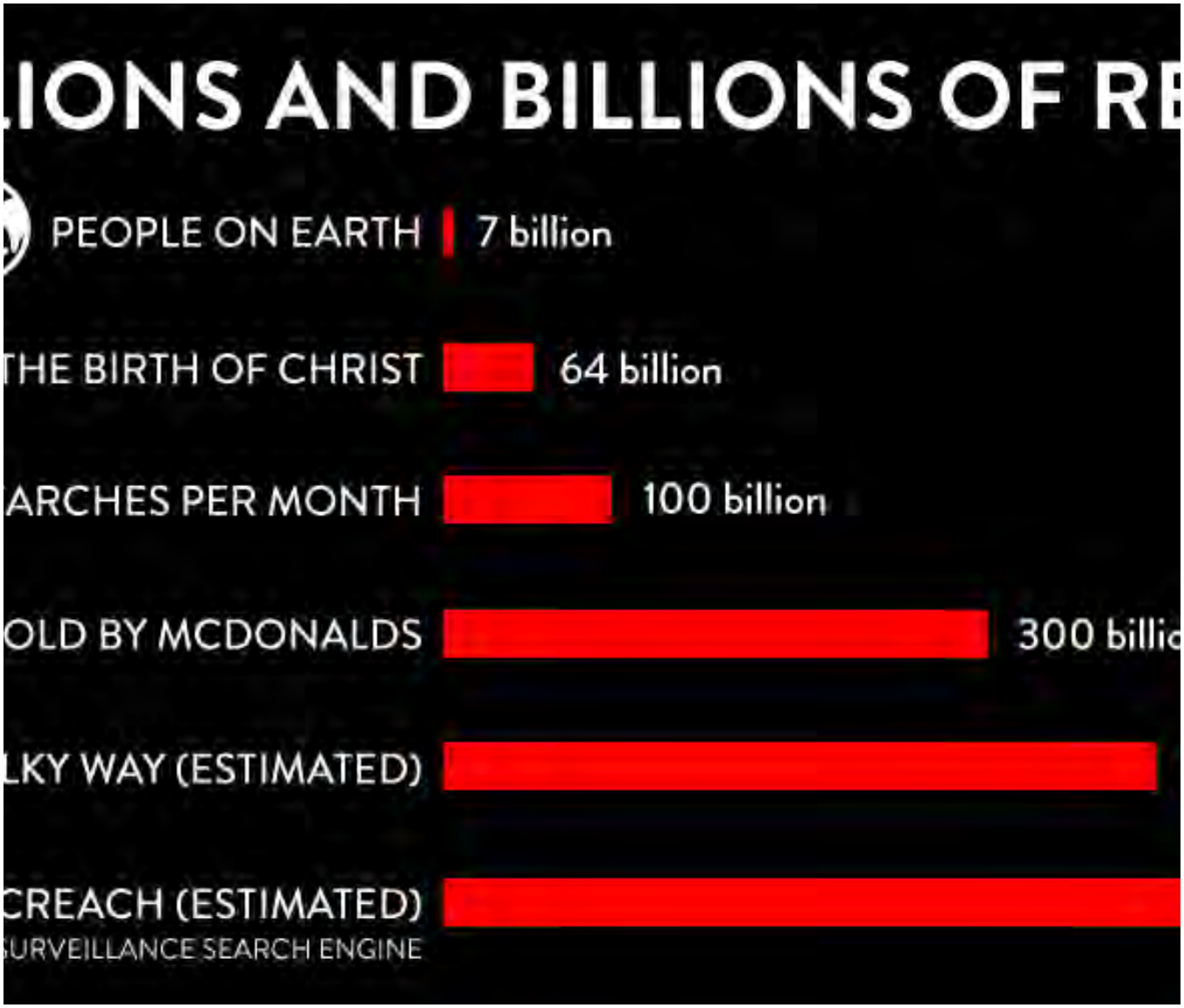
An NSA memo noted that PROTON could identify people based on whether they behaved in a "similar manner to a specific target." The memo also said the system "identifies correspondents in common with two or more targets, identifies potential new phone numbers

when a target switches phones, and identifies networks of organizations based on communications within the group." In July 2006, the NSA estimated that it was storing 149 billion phone records on PROTON.

According to the NSA documents, PROTON was used to track down "High Value Individuals" in the United States and Iraq, investigate front companies, and discover information about foreign government operatives. CRISSCROSS enabled major narcotics arrests and was integral to the CIA's rendition program during the Bush Administration, which involved abducting terror suspects and flying them to secret "black site" prisons where they were brutally interrogated and sometimes tortured. One NSA document on the system, dated from July 2005, noted that the use of communications metadata "has been a contribution to virtually every successful rendition of suspects and often, the deciding factor."

However, the NSA came to view CRISSCROSS/PROTON as insufficient, in part due to the aging standard of its technology. The intelligence community was sensitive to criticism that it had failed to share information that could potentially have helped prevent the 9/11 attacks, and it had been strongly criticized

for intelligence failures before the invasion of Iraq in 2003. For the NSA, it was time to build a new and more advanced system to radically increase metadata sharing.



A New Standard

In 2006, NSA director Alexander drafted his secret proposal to then-Director of National Intelligence Negroponte.

Alexander laid out his vision for what he described as a "communications metadata coalition" that would be led by the NSA. His idea was to build a sophisticated new tool that would grant other federal agencies access to "more than 50 existing NSA/CSS metadata fields contained in trillions of records" and handle "many millions" of new minimized records every day – indicating that a large number of Americans' communications would be included.

The NSA's contributions to the ICREACH system, Alexander wrote, "would dwarf the volume of NSA's present contributions to PROTON, as well as the input of all other [intelligence community] contributors."

Alexander explained in the memo that NSA was already collecting "vast amounts of communications metadata" and was preparing to share some of it on a system called GLOBALREACH with its counterparts in the so-called Five Eyes surveillance alliance: the United Kingdom, Australia, Canada, and New Zealand.

ICREACH, he proposed, could be designed like GLOBALREACH and accessible only to U.S. agencies in the intelligence community, or IC.

A top-secret PowerPoint presentation from May 2007 illustrated how ICREACH would work – revealing its "Google-like" search interface and showing how the NSA planned to link it to the DEA, DIA, CIA, and the FBI. Each agency would access and input data through a secret data "broker" – a sort of digital letterbox – linked to the central NSA system. ICREACH, according to the presentation, would also receive metadata from the Five Eyes allies.

The aim was not necessarily for ICREACH to completely replace CRISSCROSS/PROTON, but rather to complement it. The NSA planned to use the new system to perform more advanced kinds of surveillance – such as "pattern of life analysis," which involves monitoring who individuals communicate with and the places they visit over a period of several months, in order to observe their habits and predict future behavior.

The NSA agreed to train other U.S. government agencies to use ICREACH. Intelligence analysts could be "certified" for access to the massive database if they required access in support of a

given mission, worked as an analyst within the U.S. intelligence community, and had top-secret security clearance. (According to the latest government figures, there are more than 1.2 million government employees and contractors with top-secret clearance.)

In November 2006, according to the documents, the Director of National Intelligence approved the proposal. ICREACH was rolled out as a test program by late 2007. It's not clear when it became fully operational, but a September 2010 NSA memo referred to it as the primary tool for sharing data in the intelligence community. "ICREACH has been identified by the Office of the Director of National Intelligence as the U.S. Intelligence Community's standard architecture for sharing communications metadata," the memo states, adding that it provides "telephony metadata events" from the NSA and its Five Eyes partners "to over 1000 analysts across 23 U.S. Intelligence Community agencies." It does not name all of the 23 agencies, however.

The limitations placed on analysts authorized to sift through the vast data troves are not outlined in the Snowden files, with only scant references to oversight mechanisms. According to the documents, searches performed by analysts are subject to auditing by the agencies for which

they work. The documents also say the NSA would conduct random audits of the system to check for any government agents abusing their access to the data. *The Intercept* asked the NSA and the ODNI whether any analysts had been found to have conducted improper searches, but the agencies declined to comment.

While the NSA initially estimated making upwards of 850 billion records available on ICREACH, the documents indicate that target could have been surpassed, and that the number of personnel accessing the system may have increased since the 2010 reference to more than 1,000 analysts. The intelligence community's top-secret "Black Budget" for 2013, also obtained by Snowden, shows that the NSA recently sought new funding to upgrade ICREACH to "provide IC analysts with access to a wider set of shareable data."

In December last year, a surveillance review group appointed by President Obama recommended that as a general rule "the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes." It also recommended that any information about

United States persons should be "purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others."

Peter Swire, one of the five members of the review panel, told *The Intercept* he could not comment on whether the group was briefed on specific programs such as ICREACH, but noted that the review group raised concerns that "the need to share had gone too far among multiple agencies."

– – –

Photo credit: Alexander: Carolyn Kaster/AP Photo; CIA Headquarters: Greg Mathieson/Mai/Mai/The LIFE Images Collection/Getty Images

– – –

Documents published with this article:

- CIA Colleagues Enthusiastically Welcome NSA Training
- Sharing Communications Metadata Across the U.S. Intelligence Community
- CRISSCROSS/PROTON Point Paper
- Decision Memorandum for the DNI on ICREACH
- Metadata Sharing Memorandum

- Sharing SIGINT metadata on ICREACH
- Metadata Policy Conference
- ICREACH Wholesale Sharing
- Black Budget Extracts

CONTACT THE AUTHOR:

Ryan Gallagher
ryan.gallagher@theintercept.com
@rj_gallagher

266 Comments (closed)