Amy Baggio, OSB #01192
amy@baggiolaw.com
Baggio Law
621 SW Morrison, Suite 1025
Portland, OR 97205
Tel: (503) 222-9830
Fax: (503) 274-8575

John S. Ransom, OSB #742655
john@ransomblackman.com
Ransom Blackman LLP
1001 SW 5th Ave., Suite 1400
Portland, OR 97204
Tel: (503) 228-0487
Fax: (503) 227-5984

Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**Case No. 3:12-cr-659-MO**
Plaintiff,	
v.	**MOTION TO COMPEL NOTICE OF SEARCHES & SEIZURES AND PURPORTED LEGAL AUTHORITY FOR SEARCHES & SEIZURES**
REAZ QADIR KHAN,	
Defendant.	*ORAL ARGUMENT REQUESTED*

The defendant, Reaz Qadir Khan, through counsel, hereby moves this Court for an Order compelling notice of searches and seizures and for the purported legal authority for searches and seizures by the government. This motion for notice is based on the Fourth, Fifth, and Fourteenth

Amendments to the U. S. Constitution, as well as 18 U.S.C. § 3504, 50 U.S.C. § 1806 and 50 U.S.C. §1881(e). This Motion incorporates by reference the Memorandum in Support, filed herewith.

Respectfully submitted on July 14, 2014.

/s/ Amy Baggio
Amy Baggio, OSB #01192
503-222-9830
Of Attorneys for Defendant Reaz Khan

Amy Baggio, OSB #01192
amy@baggiolaw.com
Baggio Law
621 SW Morrison, Suite 1025
Portland, OR 97205
Tel: (503) 222-9830
Fax: (503) 274-8575

John S. Ransom, OSB #742655
john@ransomblackman.com
Ransom Blackman LLP
1001 SW 5th Ave., Suite 1400
Portland, OR 97204
Tel: (503) 228-0487
Fax: (503) 227-5984

Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**Case No. 3:12-cr-659-MO**
Plaintiff,	**MEMORANDUM IN SUPPORT OF MOTION TO COMPEL NOTICE OF SEARCHES & SEIZURES AND PURPORTED LEGAL AUTHORITY FOR SEARCHES & SEIZURES**
v.	
REAZ QADIR KHAN,	
Defendant.	

Table Of Contents

Table Of Contents

Table Of Authorities

Cases

Table Of Authorities

Statutes, Orders & Rules

Table Of Authorities

Legislative History

Other Materials

I. Introduction

The U.S. government has been spying on Reaz Khan for years. Since at least 2009, and perhaps going back to 2005 or earlier, the government has surreptitiously listened to his phone calls, read his email, monitored his internet activity, intercepted and inspected mailed parcels, looked through his luggage, and took photographs of his address books and telephone contacts.

The government has provided in discovery over 37,000 pages of PDFs, hundreds more pages of html/http internet browsing information, and sixty-four recorded phone calls. The government filed notice with this Court that the government obtained, and intends to use in this proceeding, evidence obtained and derived from the Foreign Intelligence Surveillance Act (FISA) (CR-7) and the FISA Amendments Act (FAA) (CR-59). The defense is also able to discern from discovery that the government obtained evidence by utilizing a Fed. R. Crim. P. 41 search warrant and National Security Letters. The government has refused, however, to disclose (1) the existence of additional searches or seizures or (2) the specific legal authority on which the government has relied to justify the multitude of seizures that took place over its investigation. This Memorandum supports Mr. Khan's request for disclosure of the searches and seizures to which the government has subjected him, and for notice of the specific purported legal authority for those searches and seizures.

More specific notice is required for three reasons. First, the Constitution and relevant federal statutes require the government to provide a criminal defendant with notice of any

investigative events that could constitute searches and seizures that infringed on his interests, as well as the purported lawful authority for those searches/seizures. Second, by relying on the fruits of the classified investigation in an application for a Rule 41 Search Warrant, the government exposes the sources to ordinary rules of discovery in criminal cases. Third, requiring the government to provide the requested notice will significantly advance judicial efficiency and the interests of justice by allowing the defense to focus litigation on the subsections of the statutes actually used by the government and based on the version of that statute/rule/order that was in effect at the time of the search or seizure. Otherwise, Mr. Khan will be required to conduct a full-scale challenge to every section, and subsection, of every possible statute/rule/order that the government might have used during the course of its investigation. While security concerns exist over disclosure of the contents of applications, orders, and other documents in national security cases, this motion seeks disclosure only of (1) the search/seizure events themselves and evidence obtained from them and (2) the specific purported legal authority for each of the searches/seizures. This motion also asks the Court to direct the government to connect the search/seizure events to the evidence obtained or derived from each event.

II. Tools For Evidence Collection In National Security Cases

The government has a myriad of tools to collect evidence in national security investigations, including, *inter alia*, the Foreign Intelligence Surveillance Act (FISA), FISA Amendments Act (FAA), Executive Order (EO) 12333, the Warrantless Wiretapping Program/Terrorist Surveillance Program (TSP), and National Security Letters (NSLs).

FISA establishes detailed and complex processes for a variety of information gathering activities. FISA sets forth processes for the *collection of electronic information* both authorized by the Attorney General (AG) without a court order and with an order issued by the Foreign Intelligence Surveillance Court (FISC) (Subch. I, 50 U.S.C. §§ 1801-1812), for *physical searches* authorized by the AG without a court order and with a FISC order (Subch. II, 50 U.S.C. §§ 1821-1829), for use of *pen registers and trap and trace devices* both by the AG without a court order and pursuant to an order issued by the FISC (Subch. III, 50 U.S.C. §§ 1841-1846), and for accessing *certain business records* with a FISC order (Subch. IV, 50 U.S.C. §§ 1861-1862). Since becoming law in 1978, FISA has been amended in 1999, 2001, 2004, 2006, 2008, and 2010.

The **FAA** sets forth an extensive and complex statutory scheme detailing the gathering of a wide variety of information concerning certain persons outside the United States. (Subch. VI, 50 U.S.C. §§ 1881, 1881a-1881g). The government uses the FAA to gather telephone and email content disclosed by ISPs (PRISM) and for agencies to access directly telephone and internet content (Upstream collection).

EO 12333 was originally signed into law by President Reagan in 1981 and "establishes the framework in which our governmental and military agencies are to effectuate the process of gathering foreign intelligence and counterintelligence information, and the manner in which intelligence-gathering functions will be conducted at home and abroad." EO 12333 has been amended many times by other Executive Orders since its original inception. In its briefing to the Supreme Court in *Clapper v. Amensty Intern. USA*, 133 S. Ct. 1138, 1149 (2013),

the government alleged "that it can conduct FISA-exempt human and technical surveillance programs that are governed by Executive Order 12333. *See* Exec. Order No. 12333, §§ 1.4, 2.1–2.5, 3 CFR 202, 210–212 (1981), reprinted as amended, note following 50 U.S.C. § 401, pp. 543, 547–548."[1] In the March 2014 Privacy and Civil Liberties Oversight Board (hereafter PCLOB) hearings on the FAA, Robert Litt, General Counsel, Office of the Director of National Intelligence stated: "Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated. There's a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons." PCLOB, March 19, 2014, transcript at 81. *See also* Spencer Ackerman, *NSA reformers dismayed after privacy board vindicates surveillance dragnet*, THE GUARDIAN (July 2, 2014) (describing how PCLOB would next hold hearings to evaluate the lawfulness of EO 12333 and noting: "The NSA relies upon that [EO 12333] for, among other things, its surreptitious collection of unencrypted information transiting from Google and Yahoo data centers."). Despite this tool's existence for over thirteen years, no case law exists evaluating its constitutionality.[2]

Shortly after September 11, 2001, President Bush established a **Warrantless Wiretapping Program, also known as the Terrorist Surveillance Program (TSP)** which

[1]The *Clapper* Court noted that it did not reach the issue of whether EO 12333 existed as an alternative to FAA for collection of such information. 133 S. Ct. at 1149.

[2] Plaintiffs attempted to challenge the constitutionality of EO 12333 in *United Presbyterian Church in U.S.A. v. Reagan*, 557 F.Supp. 61 (D.C.D.C. 1982) and *Halkin v. Helms*, 690 F.2d 977 (D.C.Cir.1982), but courts in both cases found the plaintiffs lacked standing.

"authorized the National Security Agency (NSA) to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States and a participant in the call was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization," *Clapper*, 133 S. Ct. at 1143-44. *See also American Civil Liberties Union v. National Sec. Agency*, 493 F.3d 644 (6th Cir. 2007) (dismissing civil challenge to TSP for lack of standing and noting TSP electronic surveillance independent of FISA). The government began obtaining surveillance under TSP in 2001; the program was purportedly discontinued in 2007. The defense is aware of no case evaluating the lawfulness of TSP.

NSLs are another tool used by the government to gather evidence in national security investigations. Five different federal statutory frameworks exist for issuance of National Security Letters. *See* 18 U.S.C. §§ 2709, 3511; 12 U.S.C. § 3414; 15 U.S.C. §§ 1861u & 1861v; 50 U.S.C. § 436. Section 2709, as amended by the USA PATRIOT Act of 2001, authorizes the Federal Bureau of Investigation (FBI) to "request the name, address, length of service, and local and long distance toll billing records of a person or entity" if the FBI asserts in writing that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities…." 18 U.S.C. § 2709(b). The provision authorizes the FBI to issue such requests to "electronic communication service providers." 18 U.S.C. § 2709(a).

Other possible sources of government surveillance in national security cases documented in the public record include **agency subpoenas**, **mail covers** (39 C.F.R. §233.3), the

Authorization to Use Military Force (AUMF), and other claims of power under the **President's Article II authority as Commander in Chief** (outside of FISA).

On the whole, each of these laws, regulations, and orders is highly complex and provides for a multitude of processes depending on a wide variety of underlying circumstances. They are amended frequently and therefore the version in effect at the time of the search/seizure is crucial in considering possible litigation as to the lawfulness of the seizure pursuant to that law/rule/order, whether as a constitutional challenge or as a challenge to whether the government adhered to the process set forth in the particular law/regulation/order.

III. Facts

Review of the discovery provided to date suggests that the government has engaged in many techniques in its investigation of Mr. Khan. Some seizures are known (the "knowns"); others are suspected (the "known unknowns"); still others may have taken place, but are completely unknown (the "unknown unknowns"). Because the defense is entitled to evaluate the constitutionality of seizures/searches and the evidence derived from those seizures/searches, the government should disclose a list of seizures that took place as well as the purported legal authority for each.

A. Known Searches & Seizures: "The Knowns"

The government appears to have seized evidence from 2005 until 2012 and could have done so pursuant to any number of laws/rules/orders, many of which have been amended, some multiple times, between 2005 to 2012. Understanding of the vast array of

seizures and elongated time period of surveillance is important to establish the complexity of the possible litigation should the Court not direct the government to specifically provide defendant with notice of exactly which statutes or other purported authority was used. Because of the extent of known seizures, the defense is utilizing a chart to delineate known seizures.

Type Of Search/Seizure	Description of Search/Seizure	*Possible* Purported Authority	*Minimal* Derivative Use
Electronic Surveillance, Phone Calls	Collection of audio recordings of Mr. Khan's telephone. 64 Recorded Phone Calls dated **September 2009 through January 2012.** Because possible bases for seizure of the calls may vary, the defense requests the government provide the statutory authority & version of statute used to seize calls: **A. Purely domestic calls between two US citizens (USCs)** **B. International calls between two USCs, one of whom is in US** **C. International calls between Mr. Khan (a USC) and a non-USC**	50 USC §1802 (Electronic Seizures without FISC order); 50 USC §§1804-1805 (Electronic Seizures with FISC order); 50 USC §1881a et seq. (FISA Amendments Act). EO123333	Search Warrant (SW) Application at 1, 17, 19

Type Of Search/Seizure	Description of Search/Seizure	*Possible* Purported Authority	*Minimal* Derivative Use
Electronic Surveillance: Text Message		50 USC §1802 (Electronic Seizures without FISC order, 8/29/09- 11/20/09) 50 USC §§1804-1805 (Electronic Seizures with FISC order); 50 USC §1881a et seq (FISA Amendments Act); EO123333	Unclear
Electronic Surveillance: Seizure and later Search of Emails	Over 500 emails **initially seized** perhaps by another agency; Over 500 emails, dated from at least 2005[3] and through 2012, which are **later extracted & reviewed**. These messages include: **A. Purely domestic emails between two US citizens (USCs)** **B. Emails between two USCs, one of whom is in US** **C. Emails between a USC and a non-USC** Because various laws may have been used, and because the emails were seized over the course of years, defendant asks that the government specify which law was used and which version of that law.	50 USC §1802 (Electronic Seizures without FISC order); 50 USC §§1804-1805 (Electronic Seizures with FISC order); 50 USC §1881a et seq. (FISA Amendments Act); EO12333	SW Application at 1-5, 7-16, 19-24, 29, 32 Indictment at 2, 6

[3] The search warrant application states at page 32 that authorization to collect emails existed from August 2009 to May 2012, however, messages in discovery date back to 2005.

Type Of Search/Seizure	Description of Search/Seizure	*Possible* Purported Authority	*Minimal* Derivative Use
Physical Seizure & Search: Seizure & Duplication Of Address Book and Telephone	The government took and copied Mr. Khan's personal papers and duplicated the contents of his cell phone as he entered the United States at SFO airport, **September 2009**	General authority to conduct border search; 50 USC §1802 (Electronic Seizures without FISC order); 50 USC §§1821-1825 (Physical Seizures with FISC Order, as to initial physical seizure); 50 USC §§1804-1805 (Electronic Seizures with FISC order, as to search of digital media); Emergency Authorization under Title 18 or Title 50	SW Application at 16
Physical Seizure & Search: Intercept of FedEx containing property, including an External Hard Drive	The government intercepted a package sent via FedEx to a third party that contained various items, including an external hard drive. The external hard drive was searched in **November 2009**	50 USC §§1821-1825 (Physical Seizures with FISC Order, as to initial physical seizure); 50 USC §§1804-1805 (Electronic Seizures with FISC order, as to search of digital media)	SW Application at 33

Type Of Search/Seizure	Description of Search/Seizure	*Possible* Purported Authority	*Minimal* Derivative Use
Physical Seizure & Search: Seizure & Duplication Of Address Book and Telephone	The government took and copied Mr. Khan's personal papers and duplicated the contents of his cell phone as he attempted to fly from PDX airport, **January 2010**	50 USC §1802 (Electronic Seizures without FISC order); 50 USC §§1821-1825 (Physical Seizures with FISC Order, as to initial physical seizure); 50 USC §§1804-1805 (Electronic Seizures with FISC order, as to search of digital media); Emergency Authorization to Search phone; Border search	Unclear
Physical Seizure & Search: Misc. Records	Government obtained Immigration, Email Account (such as address book contents), Internet Service Provider, PayPal and other miscellaneous records in defendant's name or in the name of other individuals (possibly considered co-conspirators by the government), dated **2005-2012**	50 USC §1802 (Electronic Seizures without FISC order); 50 USC §§1821-1825 (Physical Seizures with FISC Order, as to initial physical seizure); 18 USC §1861 (§215 of USA PATRIOT Act); NSLs; Agency subpoenas	SW Application at 6, 10, 17, 21-22, 27, 32
Physical Seizure & Search: Credit Reports	Government obtained credit reports on Mr. Khan from Equifax & Transunion, **September 2009**	18 USC §1861 (§215 of USA PATRIOT Act); NSLs; Agency subpoenas	Unclear

Type Of Search/Seizure	Description of Search/Seizure	*Possible* Purported Authority	*Minimal* Derivative Use
Physical Seizure & Search: Wire Transaction Records	Records obtained from Western Union (including records collected **sometime after Nov. 2011**); RQK0033198[4] & RQK0033209 and MoneyGram (**Aug.-Sept. 2011**; RQK0031270)	18 USC §1861 (§215 of USA PATRIOT Act); NSLs; Agency subpoenas	SW Application at 5, 27; Indictment at 7
Physical Seizure & Search: Call Detail Records	Government obtained Mr. Khan's Call Detail Records from **July 2008 through September 2011**	18 USC §1861 (§215 of USA PATRIOT Act); NSLs (RQK0000972) (search warrant application, para. 37, describing FBI analyzing Mr. Khan's toll records obtained through National Security Letters).	SW Application at 17
Electronic Surveillance: Monitoring Of Internet Usage	Initial collection of Mr. Khan's internet browsing, perhaps by another agency, or perhaps occurring in real-time **from July 2010 through May 2012**	50 USC §1802 (Electronic Seizures without FISC order); 50 USC §§1804-1805 (Electronic Seizures with FISC order) 50 USC §1881a et seq (FISA Amendments Act); EO 12333	SW Application at 32.
Physical Seizure & Search: Bank Records	Government obtained Mr. Khan's bank records in **September of 2012** (RQK0029824)	Grand Jury Subpoena (this batch of records was clearly obtained via GJ Subpoena)	Unclear
Physical Search & Seizure: Search Warrant	Seizures of a number of items, both digital and non-digital **March 2013**	Fed. R. Crim. P. 41 Warrant	Unclear

4 Defendant offers citations to discovery to assist the government in locating these materials. These items will not be offered as exhibits unless necessary based on the government's response to this request.

B. Additional Searches & Seizures: "Known Unknowns"

The defense has reason to believe that additional seizures, beyond those disclosed by the government in discovery, took place in its investigation of Mr. Khan. These known unknowns include at least five types.

First, defendant's call detail records provided in discovery establish over 8,000 phone calls during just a portion of the telephone monitoring period. The government, however, has provided only 64 calls from the 28 months of monitoring. Therefore, it is reasonable to conclude that there was additional phone monitoring not disclosed by the government.

Second, discovery related to web browsing information purportedly done by defendant is limited to certain browsing from mid-2010 to late 2011. There is presumably internet monitoring beyond that provided, especially in light of the search warrant application stating that the government monitored defendant's internet browsing from July 2010 until May 2012. RQK0000987.

Third, defense independent investigation of Mr. Khan's email suggests the existence of a large number of email messages that have not been provided in discovery and which cover an extensive period of time. *See also* Motion to Compel (request #32, p. 24).

Fourth, although Mr. Khan was not indicted until December of 2012, the government has provided no evidence of monitoring of calls after January 2011, nor call detail records after September 2011, nor any other information collected after September 2012. The government provided only one email dated post-January 2011. Logic dictates

that additional physical and electronic evidence collection continued beyond that disclosed to date by the government.

Fifth, and beyond electronic surveillance, the defense offers on information and belief that the government searched Mr. Khan's apartment when he left the United States for Yemen with his family in August of 2009.

C. Additional Searches & Seizures: "Unknown Unknowns"

Lastly, in light of information available in the public record regarding investigatory methods utilized by our government, there exist a large number of other possible surveillance techniques resulting in seizures that implicate the Constitution. *See*, Defendant's First Discovery Request (CR-45), para. 6, p. 4 (describing plethora of law enforcement techniques used in national security investigations). These unknown unknowns, both the seizures themselves and the purported authority for those seizures, should be disclosed to the defense if the government's conduct implicates defendant's privacy interests and if the information derived from such seizures became a fruit that advanced the government's investigation. *Wong Sun v. United States*, 371 U.S. 471 (1963).

IV. Constitutional And Statutory Law Support Issuance Of An Order For More Specific Notice Of Seizures And Purported Authority For Seizures

A. The Constitution Requires Notice of Investigative Events Particular Enough to Permit A Defendant To Evaluate The Legality Of Those Events

The Due Process Clause of the Fourteenth Amendment to the United States Constitution requires notice soon after a search or seizure, absent national security concerns, even in a non-criminal case. *Al-Haramain Islamic Found., Inc. v. United States Dep't of the*

Treasury, 686 F.3d 965, 986-87 (9th Cir. 2012). The government must "give sufficient notice concerning the factual and legal bases for its seizures." *Gete v. INS*, 121 F.3d 1285, 1297 (9th Cir. 1997). In a criminal case, the Due Process Clause imposes on the government a heightened obligation to provide a defendant with information material to a motion to suppress evidence obtained by or derived from a search or seizure, including evidence that would support a claim that a defendant has standing to challenge a search or seizure. *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000); *United States v. Barton*, 995 F2d 931, 935 (9th Cir. 1993); *see also People v. Luttenberger*, 784 P.2d 633, 643 (Cal. 1990) (holding that due process requires that a criminal defendant have "limited but reasonable access to information relevant to evaluating the validity of a search warrant"); *cf.* UNITED STATES DEPARTMENT OF JUSTICE, United States Attorney Manual § 9-5.001C.2 ("A prosecutor must disclose information that either casts a substantial doubt upon the accuracy of any evidence—including but not limited to witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence."). Such notice necessarily includes notice of government action that even arguably constitutes a search or seizure because that information "might have a significant bearing on the admissibility of prosecution evidence." Due process does not permit the government to decide against disclosure because its attorneys can construct a legal theory under which its action would not constitute a search or seizure that infringed on a defendant's interests.

Similarly, the Fourth Amendment requires the government to provide notice of

particular searches and seizures to a United States person close in time to the government action that constitutes a search or seizure. *Berger v. New York*, 388 U.S. 41, 58-60 (1967); *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1037 (D. Or. 2007), *vacated on other grounds*, 599 F.3d 964 (9th Cir. 2010). When the seizure occurs during a criminal investigation, notice is so important that a statutory scheme that authorizes domestic electronic surveillance but fails to require notice of a search or seizure violates the Fourth Amendment. *Berger*, 388 U.S. at 58-60. A warrant that fails to require any notice to an aggrieved person also violates the Fourth Amendment even when the government has an interest in delaying that notice for a reasonable time. *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986).

A possible exception to the notice required by the Due Process Clause and the Fourth Amendment arises if the government claims a national security justification for the failure to provide notice. *E.g.*, *In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (holding that "a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States"). However, as explained below, in a criminal prosecution, Congress and the Constitution require notice of a search or seizure even when the government initially took action to obtain foreign intelligence information using FISA. When the executive shifts gears from intelligence gathering to criminal prosecution (particularly in the prosecution of a United States person), the notice must be particular

enough to allow a defendant to evaluate whether to move to suppress evidence obtained or derived from a search or seizure even where the government retains some interest in secrecy because of national security concerns.

Here, the government has chosen to prosecute defendant. As a result, the Due Process Clause and the Fourth Amendment require the government to disclose, at a minimum, any government action that arguably constitutes a search or a seizure that infringed on defendant's privacy or possessory interests, the factual and legal bases for the search or seizure, and any evidence that the government obtained by, or that was derived from, the search or seizure. The government has not provided such notice in this case. Defendant asks this Court to order it to do so.

B. FISA Supports More Specific Notice And Disclosure

1. In FISA, Congress Deferred Notice Until After Initiation Of A Criminal Prosecution But Did Not Alter The Information Required In The Notice

Congress expressly requires the government to provide a criminal defendant with notice that the government intends to use evidence obtained or derived from FISA in a criminal prosecution:

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

50 U.S.C. § 1806(c); *see also* 50 U.S.C. § 1825(c) (setting forth same notice requirement for "any information obtained or derived from a psychical search" pursuant to FISA).[5] Congress requires the same type of notice when the government intends to use evidence obtained or derived from the FAA. 50 U.S.C. § 1881e; *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1154 (2013).

The government need not provide notice when it conducts a search or seizure pursuant to FISA, *United States v. Abu-Jihaad*, 630 F.3d 102, 123 n 24 (2d Cir. 2010), *cert den*, 131 S. Ct. 3026 (2011), but it must provide notice of the acquisition of information under FISA when its investigation transitions from foreign intelligence gathering to a criminal prosecution. *Clapper*, 133 S. Ct. at 1154. The notice must be particular enough so that "the affected person may challenge the lawfulness of the acquisition." *Clapper*, 133 S Ct at 1154 (citing FISA §§ 1806(c), 1806(e), 50 U.S.C. § 1881(e)(a)). Here, the notices provided by the government fail to provide adequate detail to allow the defendant to effectively challenge the lawfulness of the acquisition.[6]

The government's interest in protecting foreign intelligence gathering excuses notice like that required in Title III only until the government elects to criminally prosecute a person using FISA information:

---

[5] Hereafter, defendant's citation to 50 U.S.C. § 1806(c) (FISA § 1806(c)) also refers to the identical notice provision of 50. U.S.C. § 1825(c) and to the FAA notice requirement in 50 U.S.C. § 1881e that incorporates FISA § 1806(c).

[6] Mr. Khan hereby challenges the adequacy of both FISA and FAA notice in this single motion and will not be filing a separate challenge to the adequacy of the FAA Notice as he had originally intended when he submitted the Proposed Litigation Schedule. Therefore, Motion 2.B set out in the Court's Amended Litigation Schedule (CR-91) is subsumed in Motion 2.A.

> *Amici* particularly focus on the differences between the two statutes [Title III and FISA] concerning notice. Title III requires notice to the target (and, within the discretion of the judge, to other persons whose communications were intercepted) once the surveillance order expires. 18U.S.C.§2518(8)(d). FISA does not require notice to a person whose communications were intercepted unless the government "intends to enter into evidence or otherwise use or disclose" such communications in a trial or other enumerated official proceedings. 50 U.S.C. § 1806(c). *As the government points out, however, to the extent evidence obtained through a FISA surveillance order is used in a criminal proceeding, notice to the defendant is required.* Of course, where such evidence is not ultimately going to be used for law enforcement, Congress observed that '[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement.' S. REP. at12.

In re Sealed Case, 310 F.3d 717, 741 (FISA Ct. Rev. 2002) (emphasis added).

In sum, even if Due Process and Fourth Amendment values bow to the executive branch's power *to gather* foreign intelligence, the balance shifts and requires notice of searches and seizures when the executive decides to use information obtained through foreign intelligence gathering *to criminally prosecute a person*. The notice must be particular enough so that "the affected person may challenge the lawfulness of the acquisition." *Clapper*, 133 S Ct at 1154 (citing FISA §§ 1806(c), 1806(e), 1881(e)(a)).

2. The Text Of FISA Requires Particular Notice Of Information Obtained Or Derived From FISA, Not Generalized Notice That FISA Information Exists Somewhere In Discovery

The text and context of FISA §1806(c) indicates that Congress intended the prosecution to provide a criminal defendant of notice of *the information* it obtained pursuant to FISA, not a generic notice that it used FISA to obtain *some information* located somewhere in discovery. The text of FISA § 1806(c) reveals the congressional intent that notice identify the substance of "any information obtained or derived from electronic surveillance."

The government must provide the notice prior to each "trial, hearing or other proceeding" at which the government intends to use information obtained or derived from FISA or prior to each disclosure of that information. FISA § 1806(c).

Congress's instruction that the government must provide notice prior to *each* proceeding in which it intends to use or disclose FISA information strongly implies that Congress intended the government to identify the substance of the information. To put it another way, if Congress intended to permit the government to generally notify an aggrieved person that it would disclose or use FISA information at some unidentified point during the course of a criminal prosecutions, then it would have said so expressly. Instead, Congress required notice "*[w]henever* the government intends to offer into evidence of otherwise use of disclose . . . *any* information obtained or derived from" FISA. *Id.* (emphasis added).

The context of FISA § 1806(c) supports defendant's interpretation. Congress enacted FISA primarily to authorize the executive branch to obtain secret judicial approval for electronic surveillance or physical searches to gather foreign intelligence. *In re Sealed Case*, 310 F.3d at 727. However, Congress understood that the executive branch would obtain information that it may want to use in a criminal prosecution. *Id.* Congress enacted the subsections of FISA § 1806 to govern the use of that information. Those subsections require minimization procedures, FISA § 1806(a); authorization from the Attorney General, FISA § 1806(b); and notice to an aggrieved person and the court, FISA §§ 1806(c)-(d). Congress then authorized an aggrieved person to move to suppress

"the evidence obtained or derived from such electronic surveillance on the

> grounds that—
>
> (1) the information was unlawfully acquired; or
>
> (2) the surveillance was not made in conformity with an order of authorization or approval.

50 U.S.C. § 1806(e). *See also* Kris & Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2D, §29:11 (2012) ("FISA's failure to prescribe a form of notice when the government intends to use FISA information in litigation may therefore be due to Congress' recognition that the party adverse to the government will obtain the FISA-derived information in discovery or that the court presiding over the litigation will decide how much detail the government must give.").

Logically, a defendant who is an aggrieved person cannot prepare or file a motion to suppress "*the* evidence obtained or derived from" FISA on the ground that the evidence was unlawfully acquired unless the defendant has notice of *which* information was obtained by FISA pursuant to which authority in FISA. Moreover, a defendant cannot make a non-speculative argument that surveillance was not made in conformity with an order of authorization or approval unless the defendant knows, at the least, the date of the surveillance (or physical search) and the purported legal authority for surveillance. Thus, Congress's decision to expressly authorize a defendant to move to suppress *the evidence* obtained pursuant to FISA provides contextual support for defendant's interpretation of the notice provision of FISA § 1806(c) as requiring notice of (1) the search/seizure event that allowed the government to acquire the information and (2) the provision of FISA upon which the government relied to obtain the FISA information.

3. The Legislative History of FISA Shows That Congress Intended A FISA Notice To Mirror Notice Provided In Criminal Prosecutions That Do Not Involve Foreign Intelligence Information

The legislative history of FISA confirms that the government's notice under §1806(c) must identify the search/seizure event, the information the government obtained or derived from FISA, and the government's purported legal authority for the search or seizure. Senate Bill 1566 (1978) was enacted into law as FISA. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783. Before the passage of the senate bill, a conference committee inserted some sections of House Resolution 7308 (1978) into Senate Bill 1566. The notice provision in FISA § 1806(c) originated in the house resolution to allow an aggrieved person to challenge the evidence as soon as possible:

> The sentence bill provided for notification to the court when information derived from electronic surveillance is to be used in legal proceedings.
>
> The house amendments contained a comparable provision and also a provision, not contained in the senate bill, requiring notice to the aggrieved person. . . .
>
> The conference substitute adopts the house provisions. *The Conferees agree that notice should be given to the aggrieved person as soon as possible, so as to allow for the disposition of any motions concerning evidence derived from electronic surveillance*. . . .

H. R. REP. NO. 95-1720, at (1978) (Conf. Rep.), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060 (emphasis added).

The House Intelligence Committee report on H.R. 7308 explained that the notice provision that would become FISA §1806(c)—H.R. 7308 § 106—did not modify the government's obligation to provide discovery and notice of particular searches and seizures

after the government initiated a criminal prosecution against an aggrieved person:

> This section places additional constraints on Government use of information obtained from electronic surveillance and establishes detailed procedures under which such information may be received in evidence, suppressed, or discovered.
>
> . . . . .
>
> Subsections (c) through (i) set forth the procedures under which information acquired by means of electronic surveillance may be received in evidence or otherwise used or disclosed in any trial, hearing or other Federal or State proceeding. Although the primary purpose of electronic surveillance conducted pursuant to this chapter is not likely to be the gathering of criminal evidence, it is contemplated that such evidence will be acquired and these subsections establish the procedural mechanisms by which such information may be used in formal proceedings.
>
> At the outset the committee recognizes that nothing in subsection (C) abrogates the rights afforded a criminal defendant under *Brady v. Maryland*,[43] and the Jenks Act.[44] These legal principles inhere in any such proceeding and are wholly consistent with the procedures detailed here. Furthermore, nothing contained in this section is intended to alter the traditional principle that the government cannot use material at trial against a criminal defendant, and then withhold from such material at trial.[45]
>
> Subsection (c) states that no information acquired from an electronic surveillance (or any fruits thereof) may be used against an aggrieved person, as defined, unless prior to the trial, hearing, or other proceeding, or at a reasonable time prior to an effort to disclose the information or submit it in evidence, the United States notifies the court or other authority and the aggrieved person of its intent.
>
> . . . . .
>
> Subsection (e) provides a separate statutory vehicle by which an aggrieved person against whom evidence if to be or has been introduced or otherwise used or disclosed in any trial, hearing or proceeding may move to suppress the information acquired by electronic surveillance or evidence derived therefrom. . . .

---

[43] 373 U.S. 83 (1963).

[44] 18 U.S.C. 3500 et seq.

[45] *United States v. Andolschek*, 142 F2d 503 (2nd Cir. 1944).

H.R. REP NO. 95-1283, pt. 2, at 87-89 (1978).

The legislative history shows that Congress intended for FISA § 1806(c) to control the timing of the government's notice by deferring notice until the government elected to initiate a criminal prosecution using FISA information or FISA-derived information. Other than the timing of the notice, Congress did not modify the government's obligation to identify the actual information obtained or derived from electronic surveillance and any other information material to a potential motion to suppress. Congress identified the government's obligation to provide notice as deriving from statute, "tradition" (*viz.* common law concepts of due process), and the Constitution. The legislative history also shows that Congress intended the notice to be particular enough to permit a defendant to evaluate the legality of the surveillance. To do so, a defendant must know which information was obtained or derived from FISA, when it was obtained, and pursuant to what legal authority.

The case cited in footnote 45 of the House report as representing the "traditional" rule on the substance required in the notice provided by the government, *United States v. Andolscheck*, offers additional support for defendant's position. In *Andolscheck*, Judge Learned Hand described a criminal prosecution in which federal regulations prohibited the disclosure of investigative reports that described the alleged crimes committed by the defendants. The trial court had declined to order the prosecution to disclose the reports.

In Judge Hand's opinion, the Second Circuit reversed and remanded on the grounds that once the government elected to criminally prosecute the defendants, it could no longer rely on the regulations to justify non-disclosure:

> While we must accept it as lawful for a department of the government to suppress documents, even when they will help determine controversies between third persons, we cannot agree that this should include their suppression in a criminal prosecution, founded upon those very dealings to which the documents relate, and whose criminality they will, or may, tend to exculpate. So far as they directly touch the criminal dealings, the prosecution necessarily ends any confidential character the documents may possess; it must be conducted in the open, and will lay bare their subject matter. The government must choose; either it must leave the transactions in the obscurity from which a trial will draw them, or it must expose them fully. Nor does it seem to us possible to draw any line between documents whose contents bears directly upon the criminal transactions, and those which may be only indirectly relevant. Not only would such a distinction be extremely difficult to apply in practice, but the same reasons which forbid suppression in one case forbid it in the other, though not, perhaps, quite so imperatively. We hold that the regulation should have been read not to exclude the reports here in question. We cannot of course know, as the record stands, how prejudicial the exclusion may have been, but that uncertainty alone requires a new trial[.]

United States v. Andolschek, 142 F.2d 503, 506 (2d Cir. 1944).

The Supreme Court expressly relied on Judge Hand's reasoning in *Jencks v. United States*, 353 U.S. 657 (1957), the case that prompted Congress to enact the Jencks Act. In *Jencks*, the Supreme Court emphasized that the government forfeits its right to non-disclosure when it elects to criminally prosecute a person based on otherwise secret evidence:

> the Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and

> then invoke its governmental privileges to deprive the accused of anything which might be material to its defense.

Jencks, 353 U.S. at 370 (quoting *United States v. Reynolds*, 345 U.S. 1, 12 (1953)). The Jencks Act subsequently limited the Court's decision in *Jencks* by allowing the government to delay disclosure of prior statements of a government witness until after the witness testifies. *See United States v. Coppa*, 267 F.3d 132, 145 n. 10 (2d Cir 2001) (describing history of the Jencks Act). But of course, the Jencks Act yields to the government's *Brady* obligations if the prior statements are impeachment material or otherwise material to the defense. *Id.* at 146. In that way, Congress's intent in enacting the Jencks Act parallels Congress's intent in the notice provisions in FISA. Congress allowed the government to delay disclosure but it did not alter the substance of the required disclosure after the government initiates a criminal prosecution.

The text, context, and legislative history of FISA § 1806(c) confirm that Congress intended the government's notice to identify the information obtained or derived from FISA. It also confirms that Congress intended to incorporate the "traditional" notice requirement described by Judge Learned Hand in *Andolschek* as well as Due Process Clause and Fourth Amendment jurisprudence in *Brady* and its progeny and *Berger*. In this circuit, to comply with its *Brady* obligation, the government must disclose any information material to a defendant's motion to suppress evidence. *Gamez-Orduno*, 235 F.3d at 461. At a minimum, that requires the government to identify (1) search/seizure events and the information derived from those events and (2) disclose the provision of FISA relied on in

each search/seizure event. That information is the minimum required for a defendant to evaluate whether to move to suppress the evidence on the grounds enumerated in FISA § 1806(e).

C. Title 18 U.S.C., Section 3504 Supports More Specific Disclosure

Under Title 18, Section 3504, if a party in a proceeding before any court claims that "evidence is inadmissible" because "it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act" then the government must "affirm or deny the occurrence of the alleged unlawful act." The statute goes on to state that "'unlawful act' means any act the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto." Therefore, all electronic surveillance as discussed in this Motion would be included under §3504. Section 3504 became law in 1970, eight years prior to FISA, and requires the notice sought by defendant. *United States v. Alter*, 482 F.2d 1016, 1027 (9th Cir. 1973) (holding that a government agent's response to a defendant's claim under 18 U.S.C. § 3504(1) was insufficient because it was conclusory, failed to clearly identify all governmental agencies involved in the surveillance, failed to identify the date ranges of the surveillance, and relied on vague hearsay recitations). Accordingly, more specific disclosures of seizures and the purported legal authority for those disclosures is consistent with §3504 to allow further consideration of the lawfulness of the government's methods.

V. The Government Must Provide Defendant With Information Regarding The Searches and Seizures Used To Obtain The Information Relied Upon In the Search Warrant Affidavit

When, as in this case, the government uses information obtained through prior searches and seizures in an application for a search warrant under Federal Rule of Criminal Procedure 41, then the government must provide a defendant with information about those searches and seizures. Even when some government secrecy is reasonable under the Fourth Amendment, the Fourth Amendment requires the government to disclose to a defendant information material to determining the legality of a search or seizure after the government chooses to use that evidence in a criminal prosecution. *Freitas*, 800 F.2d at 1456.

When the government obtains search warrant, a defendant has a right to challenge the information relied upon by the government in the search warrant affidavit. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978) (recognizing a defendant's Fourth Amendment right to challenge affiant's statements upon preliminary showing); *see also United States v. Daoud*, No. 14-1284, slip op at 14-35, 2014 U.S. App LEXIS 11140 (7th Cir. June 16, 2014) (Rovner, J., concurring) (discussing the importance of balancing a defendant's rights under Franks and the government's interest in secrecy under FISA).

To imbue that right with meaning, a defendant also has a right to information about the sources of the information relied on by the government in the search warrant affidavit. *Roviaro v. United States*, 353 U.S. 53, 59 (1957) (setting forth test for a defendant to obtaining disclosure relating to a confidential informant). The government must comply with the

Fourth Amendment and the Due Process Clause by disclosing to a defendant the sources of the information relied upon in the search warrant affidavit.

Franks and *Roviaro* instruct that the government may not shield from a defendant information material to evaluating the validity of a search warrant while at the same time relying on that information to obtain a warrant. The government can omit information from a search warrant if it desires to keep the information secret. *See, e.g.,* 50 U.S.C. §§1822-1823 (authorizing physical searches pursuant to FISA); *Cf. Murray v. United States*, 487 U.S. 533, 541 (1988) (holding that a search pursuant to a warrant is lawful even if follows an earlier unlawful search of the same location so long as the government does not rely on evidence derived from the unlawful search to obtain the search warrant).

Evidence obtained pursuant to a search warrant may also be suppressed if the affiant relied on evidence obtained or derived from unlawful government action and the affidavit fails to establish probable cause absent that information. *United States v. Vasey*, 834 F.2d 782, 788 (9th Cir. 1987). Information about how the government obtained evidence in the search warrant affidavit is thus material the admissibility of evidence. The government must provide that information to a criminal defendant. Fed. R. Crim. P. 16(a)(1)(E)(i); *Barton*, 995 F.2d at 935 (holding that *Brady* applies to "a suppression hearing involving a challenge to the truthfulness of allegation in an affidavit for a search warrant"—that is, to a *Franks* hearing).

Here, the government chose to pursue a criminal prosecution using ordinary law enforcement tools, including a Rule 41 search warrant. As explained above, Agent Bowen's

affidavit in support of the search warrant relied on myriad unidentified sources, including unspecific "court-authorized surveillance" and conversations with other intelligence and law enforcement personnel.

The affiant's reliance on those sources to establish probable cause exposes the sources to ordinary rules of discovery in criminal cases. Fed. R. Crim. P 16(1)(E)(i); *United States v. Price*, 566 F.3d 900, 913 n.14 (9th Cir. 2009); *United States v. Sedaghaty*, 728 F.3d 885, 901-905 (9th Cir. 2013). The affiant's reliance on "court-authorized surveillance" and other unidentified sources also prevents the government from claiming that the sources of its evidence are privileged. Accordingly, the government must provide defendant with that information even if FISA or some other provision of law would ordinarily exempt the information from disclosure.

VI. Specific Notice Will Significantly Advance The Interests Of Justice By Allowing Defendant To Prepare Focused Motions Instead Of Motions Challenging All Potential Sources Of The Government's Evidence

In a "typical" criminal case, a defendant receives such notice when the government serves the defendant with a warrant or through investigative reports in discovery that describe any warrantless searches or seizures. When the government conducts a search or seizure pursuant to a warrant, a warrant application and the warrant itself set forth the purported legal authority for the search or seizure and thus allow a defendant to evaluate the legality of the action and seek a remedy, if necessary.

Here, most of the factual and legal sources of the government's evidence remain hidden from the defense. Without adequate notice, the defense will be forced to challenge

each piece of evidence and the facial legality of every possible law/rule/or order that might be the source of each piece of evidence, in each of the law/rule/orders various incarnations during this multi-year investigation. This result will be many hours spent researching and writing lengthy motions that ultimately may have no applicability to the government's conduct in this case. Such an approach flies in the face of judicial economy and the interests of justice.

VII. Conclusion

For the reasons set forth above, Mr. Khan seeks disclosure of (1) each search/seizure and the evidence obtained from each search/seizure and (2) notice of the purported lawful authority for each seizure/search conducted in this case.

Respectfully submitted on July 14, 2014.

/s/ Amy Baggio
Amy Baggio, OSB #01992
503-222-9830
Of Attorneys for Defendant Reaz Khan