Amy Baggio, OSB #011920
amy@baggiolaw.com
Baggio Law
621 SW Morrison, Suite 1025
Portland, OR 97205
Tel: (503) 222-9830
Fax: (503) 274-8575

Attorney for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**CR No. 3:16-cr-00061-MO**
Plaintiff,	
v.	**DEFENDANT'S MEMORANDUM IN SUPPORT OF MOTION TO COMPEL NOTICE OF SURVEILLANCE AND FOR PRODUCTION OF RELATED DISCOVERY**
JOSEPH O'SHAUGHNESSY,	
Defendant.	

I. Introduction

Joseph O'Shaughnessy and twenty-five other defendants are charged in the District of Oregon in relation to a protest at the Malheur National Wildlife Refuge (MNWR) in early 2016. The nature of the case has been set forth in numerous documents to this Court and will not be repeated here. With this motion, Defendant O'Shaughnessy provides the legal and factual basis for his request that the Court direct the government (1) to provide notice of its use of Executive

Order 12333 – whether for gathering intelligence or to obtain evidence for use in this criminal prosecution, and (2) to delineate the fruits of any such surveillance. This motion also requests that in order to ensure proper notice is given, the Court direct USAO to inquire, and investigating agencies to disclose, any use of EO12333 in investigating these defendants. As examined herein, this request is based important, emerging questions raised by a number of former Executive Branch officials and public organizations giving rise to concerns about the lawfulness of the Executive Branch's use of EO12333 to seize and search communications and over subsequent use of that evidence – either directly or indirectly – in criminal cases. Such notice is proper under 18 U.S.C. §3504 and necessary to allow the defendants to enforce and protect their rights under the Fourth, Fifth, and Sixth Amendments.

II. Request For Notice Of Surveillance & Seizures

Defendants are entitled to know how the government monitored their communications and activities, and then to test—in an adversarial proceeding—whether the government's evidence is derived from that surveillance. *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972); *Alderman v. United States*, 394 U.S. 165 (1969). More specifically, upon a claim by defendants that either direct or derivative evidence was the subject of an unlawful seizure, the government must confirm or deny the existence of that purported unlawful seizure:

> (a) In any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority of the United States–
>
> (1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act;
> ....

18 U.S.C. § 3504. Most cases regarding §3504 practice and procedure exist in the context of grand jury proceedings; however, case law suggests that in order to compel the government to respond to a § 3504 request for notice, the defendant must provide some evidence as to the basis for the claim that illegal seizures have taken place. *United States v. Alter*, 482 F.2d 1016, 1025-26 (9th Cir. 1973). Once the defendant's burden is met, the government must "affirm or deny" the existence of illegal electronic or other surveillance. *Id.* In accordance with defendants' initial burden to establish the likelihood of illegal seizures, Mr. O'Shaughnessy offers a Factual Basis, set forth in Section III, *infra*.

Before proceeding to the factual basis, however, defendants note that the government may attempt to avoid disclosure of such techniques through the process of "parallel construction." As recently described by Human Rights Watch, "'parallel construction,' ... involves creating an alternative explanation for how the authorities discovered a certain fact (and thereby hiding the true origins of warrantless evidence from defendants and judges)". Human Rights Watch, *Dispatches: US Surveillance Court Opinion Shows Harm to Rights* (22 Apr. 2016) (describing government "use" of data seized under §702 FISA in the investigations of "any federal crime" but noting apparent policy of non-disclosure to criminal defendants).[1] *See also* Shiffman & Cooke, *Exclusive: U.S. directs agents to cover up program used to investigate Americans*, Reuters (8 Aug. 2013) ("federal agents are trained to 'recreate' the investigative trail to effectively cover up where the information originated....").[2] Similarly, the FBI appears to have an *internal*

[1]Available at https://www.hrw.org/print/289188 *last visited* 10 May 2016.

[2]Available at http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805 *last visited* 10 May 2016.

policy against disclosing surveillance techniques to prosecutors in order to avoid potential disclosure to the Court or criminal defense attorneys. B. Heath, *FBI warned agents not to share tech secrets with prosecutors*, USA TODAY (20 Apr. 2016).[3] As quoted in the article, a former head of the FBI's Minneapolis Field Office said of the FBI non-disclosure policy: "The point is that there's usually no need for the case agents or the prosecutors to know how something was done." *Id.* Such a policy emphasizes the need for Court intervention to address the problem of parallel construction and to assure proper disclosures. Accordingly, Mr. O'Shaughnessy requests that the Court direct the USAO to inquire, and the FBI/other involved agencies to fully disclose, whether EO12333 was used directly or indirectly against these defendants.

III. Factual Basis For This Motion

Joseph O'Shaughnessy is no terrorist. However, government disclosures in this case establish that some elements of our government consider him and other individuals involved in the MNWR protest to be "domestic terrorists." EO12333 (described below) is a major tool used by the Executive Branch to investigate threats to national security. Accordingly, defendant moves for this request for notice and discovery.

In addition to the specific information in this case, public disclosures regarding the government's use of EO12333 to seize American citizens' communications and related rules that require sharing of that information with other agencies for use in criminal investigations further underlie this request for notice and discovery.

---

[3]http://www.usatoday.com/story/news/2016/04/20/fbi-memos-surveillance-secrecy/83280968/ *last visited* 29 Apr. 2016.

A. Evidence That The Government Considers These Defendants "Domestic Terrorists"

1. The Bunkerville Incident, April 2014

In April of 2014, Cliven Bundy was in the thick of a dispute with the Bureau of Land Management (BLM) over the impounding of his cattle for unpaid grazing fees. Bundy supporters gathered in Bunkerville, Nevada to protest what they believed were unlawful actions by the BLM. Mr. O'Shaughnessy, who had never met Mr. Bundy, viewed online reports[4] that purported to show BLM employees throwing a 57 year-old woman to the ground and releasing a police dog on a pregnant woman during the protests. After seeing the video, Mr. O'Shaughnessy went to Bunkerville over concerns about the BLM's use of excessive force on protesters. He was present on April 14, 2016, during what has been referred to as "the standoff" between Bundy supporters and the BLM (hereafter "Bunkerville incident").[5]

On April 18, 2014, Senator Harry Reid called Mr. Bundy's supporters "domestic terrorists."[6] He repeated this claim in April of 2016 when he referred to the MNWR occupation as a "particular episode of domestic terrorism [that] has roots in Nevada." Reid, *We Must Protect*

---

[4] *See, e.g.,* http://www.infowars.com/feds-assault-cancer-victim-pregnant-woman-in-clash-with-bundy-supporters/, *last visited* 1 May 2016.

[5] Mr. O'Shaughnessy currently faces federal criminal charges in the District of Nevada in relation to the Bunkerville incident. D. Nev. Case 2:16-cr-00046.

[6] *See* Fox News, Megyn Kelly, 4/18/2014, available at https://www.youtube.com/watch?v=NVJy3CBdZYY&nohtml5=False, *last visited* 04/08/2016.

Nevada's Gold Butte, Lands Across America (April 7, 2016).[7] These public statements provide proof that government officials such as Senator Harry Reid, Senate Democratic Leader and member of the Senate Select Committee on Intelligence, consider people associated with the MNWR protest "domestic terrorists."

2. Discovery References To "Domestic Terrorism"

Review of the initial 24,500 pages of discovery reveals multiple law-enforcement references that suggest the citizens charged in this case have been labeled "domestic terrorists." For example, 17 of the charged defendants have a note in their NCIC printouts from the Terrorist Screening Center (TSC) that each is "an individual identified as having possible ties with terrorism." (*See* Bates starting pages MNWR_0004672, 4792, 4773, 4666, 4864, 4841, 4882, 4782, 4678, 4768, 4857, 4915, 4909, 4752, 4729, 4706, 4893.)[8]

Also in discovery is an application submitted under the All Writs Act in support of a "block and control service" for five phones used during the final days of the MNWR occupation. The application includes an allegation that the officer is submitting the request because he has probable cause that the users of the phones have committed a federal crime of terrorism, specifically citing 18 U.S.C. § 2332b(g)(5). (MNWR_0003454.)

---

[7] Harry Reid press release, 4/06/2016, *available at* http://www.reid.senate.gov/press_releases/2016-04-07-reid-we-must-protect-nevadas-gold-butte-lands-across-america#.VxzeA-L2brc, *last visited* 04/24/2016.

[8] Bates number references are provided to assist the government locating referenced discovery materials. The defendant does not expect the contents of these reports to be in dispute; therefore, the reports themselves have not been introduced as exhibits. Should the government claim the reports are not as described in this Memorandum, the defense will seek leave to supplement the record with the reports themselves.

With specific regard to Mr. O'Shaughnessy, discovery materials include his "NCIC Interstate Identification Index." (MNWR_0004825.) Included with this report, which documents Mr. O'Shaughnessy's criminal history as being limited to two prior misdemeanors, is a section marked "Caution Information" which reads: "Caution CONTACT TERRORIST SCREENING CENTER PHONE ...."

The FBI's Search Warrants executed at the MNWR in February 2016 and related property reports describe the matter as "Domestic Terrorism – Militia Extremism." (MNWR_0001914, 2866, 4039.) Similarly, the FBI file numbers on the 302 reports designate the investigation of the defendants as "266T", which refers to "Acts of Terrorism in the United States - Domestic Terrorists" and/or "100T" which refers to "Domestic Security."

The existence of these references in discovery establishes that the government has categorized the defendants as "domestic terrorists" and therefore, as analyzed below, the government may have directly used EO12333 to address "threats to national security" and may be withholding notice of such surveillance activities based on the flawed belief that if the government does not intend to use the fruits of the surveillance against the defendants, then the government need not disclose the surveillance. Even beyond these concerns specific to the case, however, broader concerns exist based on public disclosures regarding how the government is using EO12333 to gather information as to all Americans, and querying and sharing that information as relevant to ongoing criminal investigations.

B. Publicly Disclosed Information Giving Rise To Concerns Regarding The Federal Government's Pattern And Practice Of Seizing Americans' Communications

Public disclosures over the past few years have unveiled a wide array of tools used by the government in national security investigations, including Executive Order 12333.

1. Executive Order 12333

EO12333, first enacted in 1981 by President Reagan, delineates the various roles and powers of intelligence agencies, including the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), the National Security Agency (NSA), and many others. EO12333 has been amended three times since its original enactment: in 2003, 2004, and 2008. *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. A complete copy of EO12333 is provided as Exhibit A.

EO12333 Part I sets out the goals, directions, and duties of the various agencies, including a statement that special emphasis is to be placed in "detecting and countering" "[t]hreats to the [U.S.] and its interests from terrorism." (EO12333, Part 1, §1.1(d)(2)). EO12333 Part II authorizes the intelligence agencies to create policies and procedures to accomplish the EO12333 objectives absent court involvement. EO12333 permits collection, retention, and dissemination of information concerning U.S. persons that is "incidentally obtained" if said information "may indicate involvement in activities that may violated Federal, state, local, or foreign laws." EO12333, Part 2, §2.3(i).

In describing EO12333, a former State Department employee stated: "Americans should be even more concerned about the collection and storage of their communications under

Executive Order 12333 than under Section 215 [of the Foreign Intelligence Surveillance Act]."

John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans*, WASHINGTON POST (July 18, 2014) (Exhibit B).[9] As further explained by Mr. Tye, Executive Order 12333:

> authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons be suspected of wrongdoing and places no limits on the volume of communications by U.S. persons that may be collected and retained.

Exhibit B at 2. In terms of "incidental collection," Mr. Tye explained:

> A legal regime in which U.S. citizens' data receives different levels of privacy and oversight, depending on whether it is collected inside or outside U.S. borders, may have made sense when most communications by U.S. persons stayed inside the United States. But today, U.S. communications increasingly travel across U.S. borders — or are stored beyond them. For example, the Google and Yahoo e-mail systems rely on networks of "mirror" servers located throughout the world. An e-mail from New York to New Jersey is likely to wind up on servers in Brazil, Japan and Britain. The same is true for most purely domestic communications.
>
> Executive Order 12333 contains nothing to prevent the NSA from collecting and storing all such communications — content as well as metadata — provided that such collection occurs outside the United States in the course of a lawful foreign intelligence investigation. No warrant or court approval is required, and such collection never need be reported to Congress.

Exhibit B, *Meet Executive Order 12333*, at 3.

[9]For ease in reference, primary articles cited in this Memorandum are provided as exhibits.

It further appears that the government may have stored this information in a central database, available for subsequent querying by any law enforcement or intelligence agent with access. Aaron Mamiit, *Meet ICReach, the NSA Google-like surveillance search engine*, TECH TIMES (Aug. 26, 2014) (Exhibit C) (23 agencies, including FBI, access database with "records amounting to 850 billion of phone calls, cellphone locations, emails and internet chat messages"). As concluded by Mr. Tye: "I don't believe that there is any valid interpretation of the Fourth Amendment that could permit the government to collect and store a large portion of U.S. citizens' online communications, without any court or congressional oversight, and without any suspicion of wrongdoing." Exhibit B at 5. Such collection and dissemination of private, personal information absent a warrant cannot possibly comport with the United States Constitution.

The NEW YORK TIMES recently reported that the Executive Branch is currently revising internal rules to allow law enforcement agencies direct access to seized data, rather than requiring the NSA to initially filter the raw data before it is shared with other agencies. Savage, *Obama Administration Set To Expand Sharing Of Data That NSA Intercepts* NEW YORK TIMES (25 Feb. 2016) (Exhibit D). *See also* Davis, *Coalition opposes allowing NSA to share surveillance data* (8 Apr. 2016) (describing petition to prevent changes to EO12333 that would further permit sharing of raw data) (Exhibit E; including referenced petition). These actions on the part of the Executive Branch provide further proof of the need for this Court's independent consideration of the lawfulness of their investigative methods.

In March of 2016, the Brennan Center for Justice released a report entitled *Overseas Surveillance in an Interconnected World*[10] that raised similar concerns over how the Executive Branch uses EO12333. The authors laid out several questions relevant to the government's investigation in Mr. O'Shaughnessy's case:

- ...Which agencies other than the collecting agency have access to EO 12333 data?
- ...Are there any criminal cases ... where the government has relied on evidence (a) directly obtained or (b) derived from EO 12333 surveillance? ....
- ...Under what circumstances, if at all, are criminal defendants and other parties to legal proceedings notified when information obtained or derived through EO 12333 activities is used against them?

Overseas Surveillance In An Interconnected World at 37. Mr. O'Shaughnessy shares these questions and concerns, and accordingly seeks the notice and discovery sought in this motion.

2. The Attorney General's Guidelines For Domestic FBI Operations Establish The Use Of EO12333-Seized Data In Criminal Investigations

"The Attorney General's Guidelines For Domestic FBI Operations" (dated 29 Sep. 2008) state that they "do not require that the FBI's information gathering activities be differentially labeled as 'criminal investigations,' 'national security investigations,' and 'foreign intelligence investigations'" because "all of the FBI's legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national security...." Exhibit F (FBI Guidelines) at 7. Thus, according to the FBI's own guidelines, information

[10] The Brennan Center for Justice report is available at https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf, *last visited* 24 Apr. 2016.

seized as "intelligence" is available to agents investigating crime. Moreover, in describing the FBI's authority to investigate "threats to national security," the *Domestic Operations* manual invokes EO12333 as a source available to agents. Exhibit F at 7-8.

The analysis of EO12333 combined with the specific references in the FBI Guidelines document how the government is likely using "incidentally seized" communications by the defendants and perhaps surveilling the defendants directly as "national security threats." As such, the defendants have established a record as to the likelihood that national security surveillance was used by the government in this case, as well as outlining important constitutional questions as to the lawfulness of the government's searches and seizures of data and communications under EO12333. Based on this showing, the defendant hereby officially requests notice of surveillance conducted pursuant to EO12333.

IV. The *Keith* Case Squarely Controls The Question Of Whether Notice And Disclosure Of Intelligence-Related Seizures Is Required

In *Keith*, *supra*, the Supreme Court provided a comprehensive and eerily relevant outlining of tensions between national security "intelligence-gathering" investigations and Fourth Amendment guarantees. The defendants in *Keith* requested notice of electronic surveillance to determine whether the initial information seized tainted subsequent evidence the government intended to offer against the defendants at trial. 407 U.S. at 300. The government responded with an *ex parte* affidavit of the Attorney General disclosing government surveillance, but claiming any such surveillance was exempted from Fourth Amendment scrutiny because the surveillance related to the Executive Branch's investigation of possible domestic threats to

national security. *Id.* at 300-01. After recognizing the immense responsibility of the Executive Branch to maintain the safety and stability of our nation, the Court explained:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. Senator Hart addressed this dilemma in the floor debate on s 2511(3):
>
> > "As I read it—and this is my fear—we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government."
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

Id. at 313-14. In refusing to adopt an exception to the warrant requirement for surveillance "directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and ... not an attempt to gather evidence for specific criminal prosecutions", the Court explained:

> These Fourth Amendment freedoms [from searches and seizures absent a finding of probable cause by a neutral and detached magistrate] cannot properly be guaranteed if domestic security surveillances may be conducted solely within the

> discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. *Katz v. United States*, [389 U.S. 347, 515-16 (1967)](Douglas, J., concurring). But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

407 U.S. at 316-17. The Court concluded:

> But we do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

Id. at 320. *See also United States v. Freitas*, 800 F.2d 1451, 1455-57 (9th Cir. 1986) ("surreptitious entry" warrant which allowed officers to enter and observe, but take nothing, subject to Fed. R. Crim. P. 41 notice requirement "because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment.").

If the government has a huge vat of communications, data, and metadata that it seized – directly or indirectly – from U.S. Citizens without their knowledge or consent and without a warrant, and *if* the government is querying that data to further its investigations – whether for use in mere intelligence, or to develop evidence for use in trial – then the defendants have a *per*

se right under *Keith* to know about those seizures and challenge the lawfulness of the government surveillance techniques. Moreover, considering the constitutionally suspect method of wholesale seizures of information for which U.S. citizens have a reaonable expectation of privacy, notice and disclosure is required under *Brady v. Maryland* because such practices are relevant to motions to suppress and therefore critical to the notion of due process and a fair trial. *See United States v. Gamez-Orduno*, 235 F.3d 453 (9th Cir. 2000) ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different."); *Smith v. Black*, 904 F.2d 950 (5th Cir. 1990) *vacated on other grounds* 503 U.S. 930 (1992) (due process mandates disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression hearing").

V. Conclusion

Undersigned counsel concedes that under currently released documents, it is not clear whether the FBI considers itself able to engage in direct surveillance of the defendants as potential "terrorists" under EO12333. However, public disclosures establish that EO12333 has been used by the NSA to gather huge amounts of data as to all U.S. persons. Public disclosures further establish that EO12333 and the FBI Guidelines appear to allow for querying of data seized pursuant to intelligence operations and dissemination of that information to law enforcement agencies engaged in criminal investigations.

For each of the foregoing reasons, Mr. O'Shaughnessy respectfully requests that the Court direct the government to inquire as to all relevant law enforcement agencies whether the they used EO12333 – either directly or indirectly – in their investigation of these defendants. Mr. O'Shaughnessy further requests the Court direct the government to provide notice of any such use of EO12333, as well as a delineation of the fruits of that surveillance. These disclosures are necessary to enforce Mr. O'Shaughnessy's exercise of his Fourth, Fifth and Sixth Amendment rights.

Respectfully submitted on May 11, 2016.

/s/ Amy Baggio
Amy Baggio, #011920
503-222-9830
Attorney for Defendant O'Shaughnessy