UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA	:	
-against-	:	16 Cr. 398 (PAE)
SAJMIR ALIMEHMETI,	:	
Defendant.	:	

----------x

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION FOR NOTICE OF AND DISCOVERY ABOUT THE USE OF EXECUTIVE ORDER 12333 SURVEILLANCE

Federal Defenders of New York
Attorneys for Sajmir Alimehmeti
52 Duane Street - 10th Floor
New York, New York 10007
Tel.: (212) 417-8700

Sabrina P. Shroff
Sylvie Levine
Noelle E. Lyle
Of Counsel

TO: Joon H. Kim
Acting United States Attorney
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007
Attn.: Emil J. Bove, III
George D. Turner
Assistant United States Attorneys

Table of Contents

Table of Authorities

Cases

Constitutional Provisions

Statutes

Rules

Other Authorities

I. Preliminary Statement

Mr. Alimehmeti moves for an order requiring the Government to give him notice of all Executive Order ("E.O.") 12333 surveillance used in his case, and discovery about the E.O. 12333 programs used to conduct such surveillance. This notice and discovery are required under 18 U.S.C. § 3504, the Fourth and Fifth Amendments, and Federal Rules of Criminal Procedure 12(b)(3)(C) and 16(a)(1)(E)(i). Once it is received, Mr. Alimehmeti plans to argue that the E.O. 12333 surveillance used in his case violated the Fourth Amendment, and that any evidence obtained or derived from it should be suppressed.

II. Background

a. Executive Order 12333

In 1978, following years-long investigations into unlawful executive branch spying, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to govern foreign intelligence conducted inside the United States. In 1981, President Ronald Reagan signed E.O. 12333 to govern foreign intelligence surveillance conducted outside of the United States.[1] In recent years, however, the line between domestic and foreign surveillance has blurred, and along with it the line between

[1] The full text of E.O. 12333, as amended by President George W. Bush in 2004 and 2008, is available at https://www.cia.gov/about-cia/eo12333.html.

surveillance pursuant to FISA (which requires notice and judicial process) and pursuant to E.O. 12333 (which, according to the Government, can be hidden from defendants and insulated from judicial review).

The scope of E.O. 12333 surveillance is now vast.[2] And, even though it is typically conducted outside the United States and directed at foreign nationals, it can also be used when investigating United States citizens like Mr. Alimehmeti.[3] We now live in a world where our domestic internet browsing history, a document saved domestically on a cloud server, or an email sent from a person in Manhattan to a person in Brooklyn, are frequently stored in data centers abroad. We call and text and Skype friends and family in other countries using our cell phones. Our private data makes its way outside U.S. borders daily, with and without our knowledge. This

---

[2] According the NSA, "FISA only regulates a subset of NSA's signals intelligence activities. NSA conducts the majority of its [signals intelligence] activities solely pursuant to the authority provided by Executive Order (EO) 12333." NSA Legal Fact Sheet: Executive Order 12333 (June 19, 2013), *available at* https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf.

[3] *See generally* Amos Toh, Faiza Patel, & Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, BRENNAN CENTER (Mar. 16, 2016) [hereinafter B.C. Report], http://bit.ly/1UfSdMW; *Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil*, N.Y. TIMES (Aug. 13, 2014), http://nyti.ms/1u2juDt (chart describing uses of EO 12333 surveillance); Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, THE INTERCEPT (Aug. 25, 2014), http://bit.ly/1A1VFLL (describing the FBI's ability to search data gathered under EO 12333, including "it appears, millions of records on American citizens"). While most E.O. 12333 surveillance takes place overseas, a portion of it also occurs on U.S. soil. "For example, FISA's definition of 'electronic surveillance' would not cover domestic surveillance of radio communications [including cell phone communications] between a person located in the U.S. and someone located overseas, provided that U.S. persons are not intentionally targeted. . . . This prospect raises grave constitutional concerns." B.C. Report, at 14.

information can be collected in bulk, retained, and searched by the NSA and other agencies under E.O. 12333, so long as that collection is "incidental" – a term that the NSA appears to interpret quite broadly.[4] Nor is this collection a theoretical possibility.[5] Leaks, whistleblowers, and subsequent FOIA suits have shown that the NSA relies upon E.O. 12333's authority to (1) collect metadata and audio files of every cell phone call to, from and within certain countries;[6] (2) intercept the private data of hundreds of millions of Google and Yahoo customers as it is routed to

---

[4] "United States person" is defined under E.O. 12333 §3.5(k) to include U.S. citizens, known permanent residents, and most U.S. corporations. Although EO 12333 and its implementing regulations do not generally authorize the intentional targeting of U.S. persons for surveillance, they permit bulk surveillance that results in the "incidental" collection of U.S. person information. *See* Section 4.3 of the NSA's procedures, United States Signals Intelligence Directive SP0018 (Jan. 25, 2011), *available in redacted form at* https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf (allowing the retention of "[i]nformation to, from our about U.S. PERSONS acquired incidentally" to be retained and processed). Such incidental collection appears to be common. *See* John Napier Tye, *Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans*, WASH. POST (July 18, 2014), *available at* http://wapo.st/1wPuzv2.

[5] *See* Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), *available at* https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-nottargeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html ("Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to The Post, were not the intended surveillance targets but were caught in a net the agency had cast for somebody else. Many of them were Americans.").

[6] B.C. Report, *supra* note 3, at 5 ("Under a program codenamed MYSTIC, the NSA gathers information about every cell phone call made to, from, and within the Bahamas, Mexico, Kenya, the Philippines, and Afghanistan. Such information includes the numbers dialed and the date, time, and destination of each call. In the Bahamas and Afghanistan, the NSA goes even further: It gathers and stores for thirty days an audio recording of every cell phone call placed to, from, and within these countries using a system codenamed SOMALGET. . . . [T]he NSA reportedly intends to expand the program to more countries and may already have done so."); *see also* Patrick C. Toomey et al., ACLU Letter to Privacy and Civil Liberties Oversight Board (Jan. 13, 2016), at 5-7 [hereinafter ACLU Letter], *available at* https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333.

datacenters abroad;[7] (3) collect personal information from email and instant-messaging accounts, many of them belonging to Americans;[8] and (4) conduct a daily sweep for text messages from around the globe.[9]

Under E.O. 12333 § 2.3, information collected concerning Americans is to be minimized, "in accordance with procedures established by the head of the Intelligence Community element concerned . . . and approved by the Attorney General." However, these procedures permit the retention, dissemination, and use of American communications containing "foreign intelligence information," which is broadly defined.[10] It is unclear how the procedures are applied in practice, and clear that they

---

[7] Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. TIMES (Aug. 13, 2014), *available at* https://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html ("Large email companies like Google and Yahoo have built data centers abroad, where they store backups of their users' data. Mr. Snowden disclosed that in 2012 the N.S.A., working with its British counterpart, Government Communications Headquarters, penetrated links connecting the companies' overseas data centers and collected 181.3 million records in 30 days.")

[8] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), http://wapo.st/MaTqn0 ("During a single day last year, the NSA's Special Source Operations branch collected 444,743 e-mail address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers, according to an internal NSA PowerPoint presentation. Those figures, described as a typical daily intake in the document, correspond to a rate of more than 250 million a year. . . . Although the collection takes place overseas, two senior U.S. intelligence officials acknowledged that it sweeps in the contacts of many Americans. They declined to offer an estimate but did not dispute that the number is likely to be in the millions or tens of millions.").

[9] B.C. Report, *supra* note 3, at 6 ("The NSA uses a program codenamed DISHFIRE to gather the content and metadata of hundreds of millions of text messages from around the globe, and stores the information in a database that is also accessible to [British intelligence].").

[10] "Foreign intelligence" is defined under E.O. 12333 as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists." § 3.5(e); *see also* Signals Intelligence Directive SP0018, *supra* note 4, at §§ 6-7 (setting out retention and dissemination procedures); Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities: Presidential

are not always successful.[11] Intelligence agencies also appear to have a low bar for distinguishing between U.S. persons and non U.S. persons, making it possible that minimization procedures are not implemented for some Americans.[12] In certain circumstances, intelligence analysts can then run "backdoor searches" on E.O. 12333 surveillance, querying it for information about U.S. citizens and using that information in criminal investigations.[13]

E.O. 12333's numerous bulk surveillance programs have never been reviewed by a court, and are not meaningfully overseen by Congress.[14] As a result, we know little about them, or about how they are used to gather evidence of a crime. What we do know raises grave Fourth Amendment concerns. It also shows that Mr.

Policy Directive/PPD-28 §1 (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities ("Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose.").

[11] *See* Barton Gellman et al., *supra* note 5 (describing leaked surveillance files and noting that "[n]early half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents. NSA analysts masked, or 'minimized,' more than 65,000 such references to protect Americans' privacy, but The Post found nearly 900 additional e-mail addresses, unmasked in the files, that could be strongly linked to U.S. citizens or U.S. residents.").

[12] *See* B.C. Report, *supra* note 3, at 12 ("Analysts have designated targets as foreign based on, at least in part if not entirely, the fact that their e-mails were written in a foreign language; they appeared on the chat 'buddy list' of a known foreign national; or their e-mail or social media accounts were accessed via a foreign IP address."). If E.O. 12333 surveillance was used in this case, we do not know if Mr. Alimehmeti was a designated target of such surveillance, or if his communications were collected incidentally.

[13] *See* ACLU Letter, *supra* note 6, at 4.

[14] E.O. 12333 § 3.1 provides for congressional oversight. *But see* Ali Watkins, Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued, MCCLATCHY (Nov. 21, 2013) *available at* http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html (According to then-chair of the Senate Intelligence Committee Sen. Dianne Feinstein, "her committee has not been able to 'sufficiently' oversee the programs run under [E.O. 12333]. 'Twelve-triple-three programs are under the executive branch entirely.'").

Alimehmeti was particularly vulnerable to having his information collected, retained, and queried under E.O. 12333. He had loved ones abroad with whom he communicated via cell phone, making it possible that his conversations, or metadata about them, were collected. He, like many young people, used various messaging apps, social media, and email accounts. Data from those apps and accounts is likely routed and stored abroad. He travelled abroad to visit his family, likely connecting him and his online accounts with foreign nationals. This increases the risk that he was not properly designated as a U.S. person, and that his information was not minimized as it should have been. Despite Mr. Alimehmeti's American citizenship and his many years living on American soil, E.O. 12333 programs – with their scant and unevenly followed privacy protections and lack of judicial and congressional oversight – were almost certainly used to investigate him.

b. Procedural History

In its FISA notice, the Government stated that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained and derived . . . pursuant to [FISA], as amended, 50 U.S.C. §§ 1801-1813 and §§ 1821-1829." ECF No. 14. The inclusion of 50 U.S.C. § 1813 is notable here; we have not found any other FISA notice that references it.[15] Section 1813 was promulgated in December

[15] *See, e.g.*, *United States v. Young*, No. 16-CR-265 (E.D. Va. Jan. 17, 2017), ECF No. 60 (providing notice pursuant to "50 U.S.C. §§ 1801-1812 and 1821-1829"); *United States v. Elishinawy*, No. 16-CR-

2014 as Section 309 of the Intelligence Authorization Act for Fiscal Year 2015, Pub. L. 113-293. Its purpose is to limit the retention of nonpublic telephone or electronic communications of U.S. persons acquired without their consent and without legal process, including FISA legal process. 50 U.S.C. §§ 1813(a)(1); (b)(3)(A); 113 Cong. Rec. S6464 (2014), *available at* https://www.congress.gov/congressional-record/2014/12/09/senate-section/article/S6464-1.

E.O. 12333 authorizes, among other things, collection and retention, without consent, court order, or other legal process of "[i]nformation constituting foreign intelligence or counterintelligence." E.O. 12333 § 2.3(b). Thus, E.O. 12333 surveillance falls under 50 U.S.C. § 1813.

In the Government's letter to the Court dated April 17, 2017, responding to our good cause motion, it wrote:

> The Government is aware of, and has complied with, its notice and discovery obligations in this case. Section 1813 was referenced in the FISA Notice as part of a string citation to Subchapter I of the statute, which is codified at Sections 1801 through 1813 of Title 50. Thus, the Government simply intended to cite to, and provide notice of the use of, traditional Title I FISA authority. There is no other significance to the inclusion of Section 1813 in the FISA Notice other than to cite to Title I of FISA, and it was not intended to be a reference to E.O. 12,333.

0009 (D. Md. June 24, 2016), ECF No. 47 (providing notice pursuant to "50 U.S.C. §§ 1801-1812 and 1821-1829."); *United States v. Wright*, No. 15-CR-10152 (D. Mass. June 12, 2015), ECF No. 9 (providing notice pursuant to "50 U.S.C. §§ 1801-1812 and 1821-1825").

ECF No. 51, at 9. As follow up, defense counsel wrote to the Government on May 2, 2017, referencing its April 17, 2017 letter and asking it to "confirm that no evidence in this case was obtained via or derived from E.O. 12333." The Government responded, "we are not in a position to provide any more detail in response to your question."

The Government's highly unusual notice, and the above exchange, indicate that that E.O. 12333 surveillance was used to investigate Mr. Alimehmeti. He is entitled to challenge this warrantless covert surveillance on Fourth Amendment grounds. The Government must therefore give him notice, along with discovery relating to E.O. 12333 programs, so that he can mount that challenge and ensure that no evidence obtained or derived from illegal searches is used in the case against him.

III. Argument

a. The Government Must Give Mr. Alimehmeti Notice

Notice of whether E.O. 12333 surveillance was used in this case, and discovery regarding what surveillance programs were used, are required by 18 U.S.C. § 3504, the Fourth and Fifth Amendments, and Federal Rules of Criminal Procedure 12(b)(3)(C) and 16(a)(1)(E)(i).

1. Notice Is Required under 18 U.S.C. § 3504

18 U.S.C. § 3504 states that:

> (a) In any trial, hearing, or other proceeding in or before any court . . . 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*. (emphasis added)

"Unlawful act" is defined as "the use of any electronic, mechanical, or other device . . . in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto." 18 U.S.C. § 3504(b). We allege, as set out below, that any evidence obtained or derived from programs operating under E.O. 12333 is inadmissible because it was obtained in violation of the Fourth Amendment.

"[A]lthough the claim [of an unlawful act] need not be particularized, it may not be based upon mere suspicion but must at least appear to have a 'colorable' basis before it may function to trigger the government's obligation to respond under § 3504." *United States v. Pacella*, 622 F.2d 640, 643 (2d Cir. 1980) (quotation marks and citation omitted). We have a colorable basis here, provided by (1) the reference to § 1813 in the Government's FISA notice; (2) its subsequent refusal to clarify that notice; (3) the widespread collection and retention of American's information under E.O. 12333, especially when Americans communicate overseas and online as Mr. Alimehmeti frequently did; and (4) indications that backdoor searches are used to investigate Americans, and that Americans may be deemed foreign based upon foreign contacts, of which Mr. Alimehmeti had many. The Government must

therefore either confirm that E.O. 12333 surveillance was used in investigating this case, or deny it.

Any Government denial should be "based on inquiries to the relevant government agencies and requests for searches of agency files" and be "amplified to the point of showing that those responding were in a position, by firsthand knowledge or through inquiry, reasonably to ascertain whether or not relevant illegal activities took place." *United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (quotation marks and citation omitted); *see also United States v. Alter*, 482 F.2d 1016, 1027 (9th Cir. 1973) (finding the Government's response to a claim under § 3504 insufficient because it was conclusory, failed to clearly identify all governmental agencies involved in the surveillance, and failed to identify the date ranges of the surveillance). Here, at a minimum, the Government should be required to ask the FBI, NSA, and any other relevant agencies if in the course of this investigation they queried information collected under E.O. 12333, or otherwise used programs operating under E.O. 12333 to investigate Mr. Alimehmeti.

If the Government affirms that E.O. 12333 was used in this case, it then bears the burden of demonstrating that its use was lawful. *See In re Grand Jury 11-84*, 799 F.2d 1321, 1323-25 (9th Cir. 1986); *Katz v. United States*, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment —subject only

to a few specifically established and well-delineated exceptions.") (footnotes omitted). To demonstrate lawfulness, the Government must produce sufficient information about the collection, retention, and querying of Mr. Alimehmeti's information for the Court to determine whether the use of E.O. 12333 violated the Fourth Amendment. *See In re Grand Jury 11-84*, 799 F.3d at 1325.

2. Notice and Discovery Are Required under the Fourth and Fifth Amendments and by Federal Rules of Criminal Procedure 12(b)(3)(C) and 16(a)(1)(E)(i)

The due process rights grounded in the Fourth and Fifth Amendments entitle Mr. Alimehmeti to challenge the legality of E.O. 12333 surveillance and entitle him to a meaningful opportunity to seek suppression of any derivative evidence. *See, e.g.*, *Wong Sun v. United States*, 371 U.S. 471, 486-88 (1963) (describing "fruit of the poisonous tree" doctrine); *Murray v. United States*, 487 U.S. 533, 536-37 (1988) (describing the right to seek suppression of evidence "derived" from an unlawful search); *United States v. Phillips*, 540 F.2d 319, 325-26 (8th Cir. 1976) (holding that a defendant seeking to suppress the fruit of unlawful surveillance must be given a "full and fair opportunity" to meet his prima facie burden of showing that the surveillance was unlawful).

Mr. Alimehmeti cannot challenge E.O. 12333 surveillance without sufficient notice that it was used in his case, and without some knowledge of how the surveillance was conducted. Without this notice and discovery, there is no

mechanism "to provide the scrutiny which the Fourth Amendment exclusionary rule demands." *Alderman v. United States*, 394 U.S. 165, 184 (1969); *see also id.* at 184-85 ("Adversary proceedings are a major aspect of our system of criminal justice. Their superiority as a means for attaining justice in a given case is nowhere more evident than in those cases, such as the ones at bar, where an issue must be decided on the basis of a large volume of factual materials, and after consideration of the many and subtle interrelationships which may exist among the facts reflected by these records."); *Berger v. New York*, 388 U.S. 41, 60 (1967) (finding a surveillance statute unconstitutional because it lacked, among other things, a notice requirement); *United States v. Belfield*, 692 F.2d 141, 146 (D.C. Cir. 1982) (explaining, in the FISA context, that "even when the Government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the logs of the overhears to ensure that no fruits thereof are being used against him."). E.O. 12333 is insulated from judicial review, and defendants like Mr. Alimehmeti have no remedy for violations of their constitutional rights – even if those violations led to loss of liberty. *Cf. Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1154 (2013) (holding that respondents did not have standing to challenge FISA Section 702 surveillance, but noting that the provision was not insulated from judicial review because FISA required the Government to give notice if it intended to use or disclose information obtained or derived under Section 702 in judicial proceedings).

Mr. Alimehmeti is also entitled to notice and discovery under Federal Rules of Criminal Procedure 12(b)(3)(C) and 16(a)(1)(E)(i). Rule 16(a)(1)(E)(i) directs the Government turn over "item[s] material to preparing the defense" including items material to making a suppression motion under Rule 12(b)(3)(C). *See United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993) (Under Rule 16(a)(1)(c), the predecessor to Rule 16(a)(1)(E)(i), evidence "is material if it could be used to counter the government's case or to bolster a defense.").

The Government should be required to define its terms if it says that no evidence in this case was "obtained" or "derived" from E.O. 12333. Officials have told the New York Times that the Government believes that it has no legal obligation to provide notice to defendants where evidence is only "derived" – as opposed to obtained directly – from E.O. 12333. Savage, *supra* note 7 (The Government avoids using 12333 information as direct evidence in criminal cases "so as not to have to divulge the origins of the evidence in court. But the officials contend that defendants have no right to know if 12333 intercepts provided a tip from which investigators derived other evidence."). But determinations about whether evidence is "derived from" unlawful surveillance are to be made in court, not in secret by the Government. *See Alderman*, 394 U.S. at 168.

Moreover, the Government has historically hid the use of controversial surveillance programs from defendants by arguing that the connection between the

surveillance and the discovery of derivative evidence was too attenuated to merit notice and review by the defense. The DOJ's Office of Inspector General criticized the DOJ for using such arguments in CIPA submissions to conceal Government use of the controversial Stellar Wind program from criminal defendants. *See* DOJ OIG, Annex to the Report on the President's Surveillance Program (July 10, 2009), at 351, 357-59, *available at* https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf ("We found that the Department made little effort to understand and comply with its discovery obligations . . . We believe the Department should carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA . . ."); *see also* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013), *available at* http://nyti.ms/1r7mbDy (Noting that Solicitor General Donald B. Verrilli had told the Supreme Court in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, that someone would have standing to review FISA Section 702, "because prosecutors would notify people facing evidence derived from surveillance under the 2008 law. But it turned out that Mr. Verrilli's assurances clashed with the practices of national security prosecutors, who had not been alerting such defendants that evidence in their cases had stemmed from wiretapping their conversations without a warrant.").

The Government may also be relying on the fact that, under its unilateral assessment, an exception to the Fourth Amendment's warrant requirement applies in

cases having to do with foreign intelligence, or that it believes the fruit of the poisonous tree doctrine does not apply in this context. But questions about exceptions and attenuation are also not the Government's to decide. They should be resolved by a court after a defendant has notice about the origins of the Government's evidence. *See Kolod v. United States*, 390 U.S. 136, 137 (1968), *on reargument sub nom. Alderman v. United States*, 394 U.S. 165 (1969) (rejecting the DOJ's statement that surveillance produced nothing relevant to the defendant's case, and holding "[w]e cannot accept the Department's ex parte determination of relevancy in lieu of such determination in an adversary proceeding in the District Court.").

Moreover, reports in recent years have indicated that the Government often uses "parallel construction" in cases such as this one. That is, it makes evidence obtained using a secret or controversial method appear to have been obtained using a second, more orthodox method.[16] Documents leaked to Reuters show that "law enforcement agents have been directed to conceal how such investigations truly begin - not only from defense lawyers but also sometimes from prosecutors and judges. . . . [F]ederal agents are trained to 'recreate' the investigative trail to effectively cover up

---

[16] *See, e.g.*, Sarah St. Vincent, *Dispatches: New US Surveillance Guidelines May Jeopardize Rights*, Human Rights Watch (Apr. 11, 2016), *available at* https://www.hrw.org/news/2016/04/11/dispatches-new-us-surveillance-guidelines-may-jeopardize-rights; Brian Fung, *The NSA is giving your phone records to the DEA. And the DEA is covering it up.*, WASH. POST (Aug. 5, 2013), *available at* https://www.washingtonpost.com/news/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/?tid=a_inl&utm_term=.b43eab7eacc9.

where the information originated, a practice that some experts say violates a defendant's Constitutional right to a fair trial." John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), *available at* http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805.

If the Government denies using E.O. 12333 surveillance in this case, it should be required to include in its denial a statement that parallel construction was not used. It should also be required to state that its denial is based on the absence of E.O. 12333 surveillance and queries of E.O. 12333 databases in the Government's investigation of Mr. Alimehmeti – not upon its own determinations of relevancy, attenuation, or whether or not any evidence was "derived from" E.O. 12333 surveillance.

If the Government admits to using E.O. 12333 surveillance in this case, it should be ordered to provide discovery of what surveillance was used and what evidence was derived therefrom, in order to allow Mr. Alimehmeti a meaningful opportunity to challenge the legality of the surveillance and seek suppression.

b. The Use of E.O. 12333 in This Case Violates the Fourth Amendment

We are limited in making particularized allegations by the secrecy surrounding E.O. 12333 surveillance programs – a difficulty compounded by the Government's lack of notice and discovery. We outline briefly below why the use of E.O. 12333 to

collect, retain, and review Mr. Alimehmeti's information violates the Fourth Amendment. If the Government gives us notice and discovery, we intend to provide the Court with more detailed briefing.

As an initial matter, Americans like Mr. Alimehmeti clearly have a protected privacy interest in their calls, emails, and private online communications. "[B]road and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." *United States v. U.S. Dist. Court for E. Dist. of Mich. (Keith)*, 407 U.S. 297, 313 (1972). The Fourth Amendment's protection extends not just to domestic communications, but to international ones as well. *See, e.g.*, *United States v. Ramsey*, 431 U.S. 606, 616-20 (1977); *United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992).

The Supreme Court has "repeatedly held that searches conducted outside the judicial process, without prior approval by [a] judge or [a] magistrate [judge], are *per se* unreasonable ... subject only to a few specifically established and well-delineated exceptions." *City of Los Angeles, Calif. v. Patel*, 135 S. Ct. 2443, 2451-52 (2015) (citations and quotation marks omitted). None of those few, well-delineated exceptions apply here. *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008) ("[W]e hold 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."). And even if an exception did apply, the Government would still have to show that a warrantless search was reasonable – which it cannot do. *Id.* ("[E]ven though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement.").

Nor does "incidental" collection of Mr. Alimehmeti's private information insulate the Government from the warrant requirement here. Collection is not "incidental" when it is anticipated and foreseeable, as it is under E.O. 12333. *See United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157 (2d Cir. 2008) (holding that Government surveillance of a U.S. citizen abroad was not incidental because it was not "unanticipated" that his communications would be overheard); ACLU Letter, *supra* note 6, at 17 ("The volume of communications that appears to be intercepted 'incidentally' under EO 12333 dwarfs that of communications intercepted incidentally under original FISA, Title III, and likely Section 702 as well. The scale of incidental collection is a direct consequence of the fact that EO 12333 permits suspicionless targeting and bulk collection and retention.").

Finally, even if bulk collection and retention of U.S. person information under E.O. 12333 were to pass constitutional muster, the Government must obtain a warrant before querying the collected data for use in a criminal investigation. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2493 (2014) (holding that police must obtain a warrant to search cell phones seized during searches incident to arrest and noting that "the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency") (quotation marks and citation omitted). "If the Warrant Clause were held inapplicable here, then the federal intelligence machine would literally enjoy unchecked discretion." *Keith*, 407 U.S. at 325 (Douglas, J., concurring). The same danger present in the *Keith* case – the danger which Congress sought to ameliorate by setting up FISA and the FISC – is now present again in the form of foreign intelligence surveillance under E.O. 12333 that reaches the private information of American citizens.

IV. Conclusion

Courts play a crucial role in balancing security concerts against civil liberties. *See, e.g.*, *Keith*, 407 U.S. at 317 (1972) ("[T]hose charged with . . . 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."); *Johnson v. United States*, 333 U.S. 10, 14 (1948) (Fourth Amendment protection "consists in requiring that . . . inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."). This is especially true in cases like Mr. Alimehmeti's. "National security cases . . . 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." *Keith*, 407 U.S. at 313; *see also id.* at 331 ("Senator Kennedy . . . found 'the frightening possibility that the conversations of untold thousands are being monitored on secret devices.' More than our privacy is implicated. Also at stake is the reach of the Government's power to intimidate its critics. When the Executive attempts to excuse these tactics as essential to its defense against internal subversion, we are obliged to remind it, without apology of this Court's long commitment to the preservation of the Bill of Rights from the corrosive environment of precisely such expedients.") (Douglas, J., concurring).

Without notice, E.O. 12333 and the controversial programs that operate under its authority are insulated from judicial review. Defendants may have their liberty taken away without any opportunity to challenge invasions of their Fourth Amendment rights. The Court should therefore – in accordance with 18 U.S.C. §

3504, the Fourth and Fifth Amendments, and Federal Rules of Criminal Procedure 12(b)(3)(C) and 16(a)(1)(E)(i) – order the Government to give Mr. Alimehmeti specific, detailed notice of whether or not E.O. 12333 surveillance was used in his case. If affirmative notice is given, Mr. Alimehmeti is entitled to discovery about how the surveillance was used and will argue, as above, that E.O. 12333 violates the Fourth Amendment, and that any evidence obtained or derived from it should therefore be suppressed.

Dated: New York, New York
May 15, 2017

Respectfully Submitted,

_____/s/_____
Sabrina P. Shroff
Sylvie Levine
Noelle E. Lyle
Assistant Federal Defenders
52 Duane Street – 10th Floor
New York, NY 10007
(212) 417-8713