IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. JAMSHID MUHTOROV, and
2. BAKHTIYOR JUMAEV,

Defendants.

DEFENDANTS' JOINT MOTION FOR NOTICE OF THE SURVEILLANCE TECHNIQUES UTILIZED BY THE GOVERNMENT IN ITS INVESTIGATION OF SAID DEFENDANTS

JOINT MOTION

The defendants, Jamshid Muhtorov and Bakhtiyor Jumaev, by and through their counsel, move this Honorable Court to require the government to provide notice of the surveillance techniques utilized by it in its investigation of said defendants, and they inform the Court as follows:

INTRODUCTION

Recent disclosures have shown that the government uses a wide array of surveillance programs to monitor the communications and activities of its investigative targets and millions of others. Under various authorities, the government collects in bulk the content of phone calls in and out of certain countries, the content of emails, location data, electronic address books, calling records, and records of internet activity. Many of these surveillance programs are operated by the Executive Branch without congressional

or judicial oversight. They have never been reviewed by any court, let alone been the subject of public or adversarial judicial review. All of them are warrantless and conducted without a finding of individualized suspicion.

Notice of the government's reliance on these surveillance techniques is essential to the due process rights of the defendants in this case. Without notice, the defendants cannot test whether the government's evidence was, in fact, lawfully obtained—or whether government surveillance conducted without a warrant and without probable cause violated the defendants' rights. Notice of surreptitious electronic surveillance is routinely required in criminal cases. Courts confronted this question with the advent of wiretapping decades ago and concluded that the government could not criminally prosecute an individual while keeping the sources of its evidence secret. Instead, 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. *See, e.g.*, *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972); *Alderman v. United States*, 394 U.S. 165 (1969).

The government today has sought to carve out an exception to this due process requirement. The government has routinely failed to provide notice of its surveillance activities to courts and criminal defendants in cases like this one—thereby avoiding judicial review. It is withholding notice, reports show, based on a narrow interpretation of its legal obligations.

Mr. Muhtorov and Mr. Jumaev respectfully request that the Court issue an order requiring the government to provide notice of: (1) each surveillance technique it used to obtain information about the defendants' communications or activities in its

investigation; (2) the timing or duration of that surveillance; (3) the legal authority relied upon; and (4) the evidence obtained or derived from that surveillance.

I. The Government's Investigation of the Defendants

Defendants have been provided only limited discovery, but it is already clear that the government's investigations of Mr. Muhtorov and Mr. Jumaev involved extensive monitoring of their private communications and other activities. Yet the government has never explained how it obtained much of this information, let alone which legal authorities provided the basis for its surveillance of the defendants. Defendants summarize certain elements of the government's wide-ranging investigation here.

In 2005, the government designated the Islamic Jihad Union (IJU) in Uzbekistan as a terrorist organization. Muhtorov Compl. ¶ 11 (Doc. 1). Mr. Muhtorov came to the United States as a refugee in 2007; Mr. Jumaev moved to the United States in 2000. From the time that both men arrived in the United States, they communicated with others—individuals located in the U.S. and abroad—by phone, Skype, and email.

Mr. Muhtorov and Mr. Jumaev first met in November of 2009, when Mr. Muhtorov stayed at Mr. Jumaev's home in Philadelphia for several weeks while Mr. Muhtorov attended truck-driving school. Shortly after Mr. Muhtorov left Philadelphia, immigration authorities arrested Mr. Jumaev in February 2010 on the grounds that he had overstayed his visa. At that time, according to the government's criminal complaint, Mr. Jumaev provided authorities with his mobile phone number. *See* Jumaev Compl. ¶ 13 (Doc. 1, Case No. 12-mj-01039-KLM). Mr. Jumaev was released on bond from immigration custody in April 2010. Family and friends, including Mr. Muhtorov, contributed funds to help secure Mr. Jumaev's release. Soon after the time of Mr.

Jumaev's release through the beginning of 2012, the defendants communicated frequently over the phone and occasionally via Skype.

The government's criminal complaints, as well as documents that it has produced in discovery thus far, show that its investigations of the defendants have relied on extensive surveillance of their internet-based communications and activities. According to its criminal complaint, the government monitored Mr. Muhtorov's communications with the website administrator and facilitator for www.sodiqlar.com, an Uzbek language website that the government alleges is affiliated with the Islamic Jihad Union in Uzbekistan. *See* Muhtorov Compl. ¶¶ 10, 12, 15–17, 26–27. The limited discovery provided to defendants to date shows that the government intercepted communications between Mr. Muhtorov and the www.sodiqlar.com website administrator from January 2011 to January 2012. In addition, the complaint describes the government's monitoring of at least two email accounts allegedly belonging to Mr. Muhtorov. *See* Muhtorov Compl. ¶ 12. The government also tracked Mr. Muhtorov's online searches, including his use of a number of travel websites in May 2011 and January 2012. *See id.* ¶¶ 19, 31–32. Likewise, it appears to have tracked internet searches conducted by Mr. Muhtorov's wife. *See id.* ¶ 22.

The government similarly tracked and monitored Mr. Jumaev's internet communications and activities. It was aware of Mr. Jumaev's visits to www.furqon.com, a website allegedly associated with the IJU; his watching of videos on political and religious matters; and his alleged commenting on YouTube videos. *See* Jumaev Compl. ¶ 29. It has also produced intercepted communications between Mr. Jumaev and third

parties—including his wife and children—who reside in various foreign countries, including Uzbekistan.

The government likewise tracked and monitored the defendants' phone calls, including those within the United States. *See, e.g.*, Muhtorov Compl. ¶¶ 12, 14, 21–24, 28; Jumaev Compl. ¶¶ 13, 16–18, 20–26, 28. As shown by the government's productions to date, the government intercepted hundreds of phone calls between January 2011 and January 2012 that involved Mr. Muhtorov. Many of these communications were with Mr. Jumaev.

The government also tracked and monitored the defendants' financial transactions. Beginning in 2007, Mr. Muhtorov used MoneyGram and similar services to send money to individuals both inside the United States and abroad. Likewise, from the time of his arrival in the United States in 2000 through the time of his arrest in this matter in March 2012, Mr. Jumaev regularly used similar services to send money to individuals abroad. The government plainly collected financial records and information about the defendants. *See, e.g.*, Bates No. G_000303 (describing an FBI trash cover effected outside of Mr. Jumaev's residence on January 17, 2011, in which agents reported finding a MoneyGram receipt for $300). According to its criminal complaint against Mr. Jumaev, the government obtained bank records showing that a $300 check was made out to Mr. Muhtorov by a friend of Mr. Jumaev in March 2011. *See* Jumaev Compl. ¶ 35.

Although the unclassified documents produced in discovery go back no earlier than January 2011, there is reason to believe that the government was monitoring the defendants' communications and activities far earlier—even prior to January 2010, when immigration authorities commenced removal proceedings against Mr. Jumaev. Of course,

these removal proceedings did not occur in a vacuum, but likely occurred in parallel with the government's criminal investigations of each defendant. In both its criminal investigation and the removal action, the government most likely relied on information gathered through surveillance of Mr. Muhtorov—and by extension, surveillance of Mr. Jumaev—before January 2010.

II. The Government Is Withholding Notice from Criminal Defendants Based on Secret Legal Interpretations

Over the past year, it has become increasingly evident that the government is withholding notice of its reliance on controversial spying programs in criminal prosecutions. In doing so, the government is preventing defendants from challenging sweeping new forms of surveillance, often conducted without any warrant or prior judicial review. Recent reports indicate that the government holds an unjustifiably narrow view of its notice obligations, even when it relies on novel and legally untested surveillance programs in criminal prosecutions.[1]

This prosecution has already become a case-in-point for the government's failure to comply with its notice obligations. Mr. Muhtorov learned that he had been surveilled by the NSA under the FISA Amendments Act ("FAA") in October 2013—but only belatedly and only after the government had failed to provide such a notice to *any* defendant for five years. During that time, the government had avoided court review of its surveillance activities by relying on an undisclosed and "narrow understanding" of its

[1] *See, e.g.*, Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014, http://nyti.ms/1wPw6l0 ("Savage 12,333 Article").

notice obligations.[2] The government altered course last year, but only after the Solicitor General had inaccurately described the government's FAA notice policy to the Supreme Court.[3] Following public outcry, the Solicitor General apparently concluded that the Justice Department's FAA notice policy "could not be legally justified." Savage FAA Article. Mr. Muhtorov then received what the government calls a "Second FISA Notice" (Doc. 457)—more than a year-and-a-half after the government filed its original notice in this case.[4] Four other defendants around the country have also received belated notices, almost all of them *after* they had already been tried or convicted.[5]

The public record shows that the government continues to withhold notice of many other controversial surveillance programs. In particular, in a recent report,

---

[2] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, http://nyti.ms/1r7mbDy ("Savage FAA Article").

[3] *See* Savage FAA Article; Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. Times, July 15, 2013, http://nyti.ms/12ANzNM.

[4] The government has repeatedly offered misleading explanations for its long-running failure to provide notice. It has told this Court and at least three others that, prior to 2013, it had not "considered" the issue of FAA-derived evidence. *See, e.g.*, Gov't Unclassified Mem. in Opp. to Def. Mot. to Suppress Evidence at 9 n.2, *United States v. Muhtorov*, No. 12-cr-33 (D. Colo. May 9, 2014) (Doc. 559). But that is demonstrably false. The issue was brought to the attention of Justice Department lawyers at least as early as 2011, when a defendant in *United States v. Khan* filed a motion focused on this precise question. Mot. for Clarification, No. 11-cr-20331 (S.D. Fla. Dec. 14, 2011) (ECF No. 219). The issue was raised again in 2012—in the Supreme Court, by the plaintiffs in *Clapper v. Amnesty International USA*. Br. for Respondents at 58 n.22, *Clapper*, 133 S. Ct. 1138 (Sept. 17, 2012). Moreover, multiple news reports indicate that NSD attorneys *had* considered the issue long before 2013, had decided that notice of evidence derived from FAA surveillance was not required, and had taken active steps to avoid ever giving notice of FAA surveillance in criminal cases. *See, e.g.*, Savage FAA Article (explaining that NSD had "long used a narrow understanding of what 'derived from' means" to avoid providing notice).

[5] Those cases are: *United States v. Hasbajrami*, No. 11 Cr. 623 (E.D.N.Y.) (post-conviction notice); *United States v. Mihalik*, No. CR 11-833(A) (C.D. Cal.) (post-conviction notice); *United States v. Mohamud*, No. 10-cr-475 (D. Or.) (post-trial notice); *United States v. Khan*, No. 12-CR-659 (D. Or.).

government officials insisted that "defendants have no right to know" if investigators derived evidence from any of the government's sweeping surveillance activities under Executive Order 12,333. Savage 12,333 Article. That position conflicts directly with the right of defendants—under the Fourth and Fifth Amendments, and the "fruit of the poisonous tree" doctrine—to seek suppression of unlawfully obtained evidence. *See Wong Sun v. United States*, 371 U.S. 471, 486–88 (1963); *United States v. De La Cruz*, 703 F.3d 1193, 1200–01 (10th Cir. 2013). It is also clear that the government is not providing notice to criminal defendants when investigators rely on the NSA's bulk collection of phone records and email metadata. Although both of these domestic surveillance programs operated for a decade or more—and tips were routinely fed to FBI investigators—no defendant has ever received official notice from the government. *See* Sections III.B–C.

Compounding these problems, the government has refused to publicly explain its notice policies in any detail. Despite the efforts of defendants around the country, the government has refused in this case and others to disclose its view of its notice obligations.[6] There is no reason for this secrecy, except to keep courts and defendants from ascertaining whether the government is providing notice when it should be. Recent events have shown that it is not.

[6] *See, e.g.*, Def. Response at 8–16, *United States v. Qazi*, 12-cr-60298 (S.D. Fla. July 21, 2014) (ECF No. 228).

III. The Government Must Provide Notice of the Surveillance Programs It Used in Its Investigation of the Defendants

A. Surveillance Under Executive Order 12,333

There is reason to believe that some of Mr. Muhtorov's and Mr. Jumaev's communications were obtained under Executive Order 12,333, which serves as the "primary source" of the NSA's foreign intelligence-gathering authority and governs most surveillance conducted abroad.[7] According to the NSA's own documents, the agency "conducts the majority of its [signals intelligence] activities solely pursuant to" E.O. 12,333.[8] Over the past year, it has grown increasingly clear that the scale of the government's surveillance under E.O. 12,333 is vast—and that the government uses this information when investigating individuals here in the United States.[9] Under this authority, the NSA collects both content—such as phone calls, emails, and text messages—and so-called "metadata" like phone records, records of internet activity, and location information.

Recent reports show just how expansive the government's surveillance under E.O. 12,333 has become. These reports indicate that the NSA is, among other things:

- Recording and storing every single cell phone call in and out of at least two countries, including the Bahamas.[10]

---

[7] NSA Overview of Signals Intelligence Authorities, Jan. 8, 2007, at 4, http://bit.ly/1ruKbBk; *see* 3 C.F.R. 202, 210–212 (1981), reprinted as amended, note following 50 U.S.C. § 401, pp. 543, 547–548.

[8] NSA Legal Fact Sheet: Executive Order 12333, Jun. 19, 2013, at 1, http://bit.ly/1CG9EtT.

[9] *See* Savage 12,333 Article; *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 E.O. 12,333 surveillance).

[10] Ryan Devereaux et al., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, Intercept, May 19, 2014, http://bit.ly/1qFFVNC.

- Collecting communications in bulk from overseas communications hubs and from satellite transmissions.[11]
- Collecting nearly five billion records per day on the location of cell phones, including those of Americans.[12]
- Collecting hundreds of millions of contact lists and address books from personal email and instant-messaging accounts.[13]
- Surreptitiously intercepting data from Google and Yahoo! user accounts as that information travels between those companies' data centers located abroad.[14]

The full extent of the government's activities under E.O. 12,333 is unknown, but it is clear that the government intercepts and searches an enormous amount of data with these tools.[15] It is also clear that both the NSA and FBI use this information in investigations like the one that preceded this prosecution.[16] For example, one tool enables the FBI to search this data for information that "can be used to track people's movements, map out their networks of associates, help predict future actions, and potentially reveal religious affiliations or political beliefs."[17]

---

[11] Savage 12,333 Article.

[12] Brendan Sasso, *NSA Tracks Phone Locations Under Executive Order*, Hill, Dec. 6, 2013, http://bit.ly/1BOqWCZ; *see* Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, Wash. Post, Dec. 4, 2013, http://wapo.st/1mSXZAP.

[13] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post, Oct. 14, 2013, http://wapo.st/MaTqn0.

[14] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post, Oct. 30, 2013, http://wapo.st/1mSYNpm (describing "large-scale collection of Internet content" that "would be illegal in the United States").

[15] *See* Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, Intercept, Aug. 25, 2014, http://bit.ly/1A1VFLL ("Gallagher Article").

[16] *See, e.g.*, *id.* (describing FBI's ability to search data gathered under E.O. 12,333); United States Signals Intelligence Directive 18, § 7.2(c)(4) (permitting NSA to share information potentially related to criminal activity), http://1.usa.gov/1tD1kGU.

[17] Gallagher Article.

Crucially, although surveillance conducted under E.O. 12,333 takes place outside the United States, the communications of U.S. persons may still be swept up in large quantity.[18] Americans routinely place phone calls, send emails, and communicate online with people and organizations located overseas. Even purely *domestic* communications or data may be routed or stored abroad without a person ever realizing it, leaving that data vulnerable to collection under E.O. 12,333.[19]

In this case, the government has relied on, among other things, its interception of Mr. Muhtorov's international communications with the administrator of www.sodiqlar.com, a non-U.S. person located abroad; Mr. Jumaev's visits to foreign-based websites; and Mr. Jumaev's communications via phone and other electronic methods with persons overseas. It is likely that some or all of these communications were either collected pursuant to E.O. 12,333, or were collected based on information derived from earlier E.O. 12,333 surveillance.[20]

---

[18] *See, e.g.*, Savage 12,333 Article; John Napier Tye, Op-Ed, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, http://wapo.st/1wPuzv2.

[19] *See, e.g.*, Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad at 19-27*, Telecomm. Policy Research Conf. (Aug. 27, 2014), http://bit.ly/1lWB4I4.

[20] Although the FBI says that it obtained "court authorization" to acquire some of Mr. Muhtorov's emails, *see* Muhtorov Compl. ¶ 12, that is not inconsistent with the government's reliance on E.O. 12,333 to acquire the defendants' communications. For example, it is possible that the NSA first acquired Mr. Muhtorov's emails via E.O. 12,333 and subsequently tipped the FBI, which then obtained the same communications and/or others pursuant to court authorization. In that case, the government's evidence would still be derived from E.O. 12,333 surveillance of the defendant, and Mr. Muhtorov would still be entitled to notice. A similar scenario may have occurred with Mr. Jumaev. The FBI obtained Mr. Jumaev's mobile phone number as part of his immigration arrest in February 2010, which the government may then have used to query information it had already obtained under E.O. 12,333, or to collect information under other undisclosed legal authorities. *See* Jumaev Compl. ¶ 13 (claiming, without detail, that the FBI used

Surveillance programs operated under E.O. 12,333 have never been reviewed by any court. Moreover, these programs are not governed by any statute, including FISA, and, as the chair of the Senate Intelligence Committee has conceded, they are not overseen in any meaningful way by Congress.[21] Instead, this surveillance is conducted entirely under Executive Branch authority, on the basis of a presidential directive first issued by President Reagan in 1981. As a result, there are few statutory or practical constraints on the government's use of this authority, even when it sweeps in huge quantities of Americans' data overseas. As a former State Department official recently wrote, "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."[22]

Based on the public record, the government rarely provides notice to criminal defendants when its investigation has relied upon surveillance conducted under E.O. 12,333. In fact, according to unnamed government officials, the Department of Justice believes that it has no legal obligation to provide notice to defendants, at least where its

"appropriate authority" to obtain information about Mr. Jumaev "through various investigative techniques")

[21] *See* Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, McClatchy, Nov. 21, 2013, http://bit.ly/1lCXFsC.

[22] John Napier Tye, Op-Ed, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, http://wapo.st/1wPuzv2.

evidence is only "derived"—as opposed to obtained directly—from E.O. 12,333 surveillance.[23]

B. The NSA Call-Records Program

It is also extremely likely that the government's investigation of Mr. Muhtorov and Mr. Jumaev relied on its bulk collection of Americans' phone records. For more than a decade, the NSA has been collecting call records in bulk from major domestic telecommunications companies. The government conducts this program under Section 215 of the Patriot Act, 50 U.S.C. § 1861.[24] As currently operated, the government presents multiple telecommunications carriers with secret court orders requiring them to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating to every domestic and international call placed on their networks.[25] The orders, which are renewed every ninety days, further specify that the phone records sought include, for each call, the originating and terminating telephone number as well as the call's time and duration. Once collected, the bulk call records are stored in a government database for five years, where the NSA queries those records—hundreds or thousands of times each year—to search for unknown connections between its

[23] Savage 12,333 Article ("[O]fficials contend that defendants have no right to know if 12333 intercepts provided a tip from which investigators derived other evidence.").

[24] *See* Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 06-05 (FISC May 24, 2006), http://1.usa.gov/1f28pHg; *see* USA PATRIOT Act of 2001, Pub. L. 107-56.

[25] Secondary Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISC Apr. 25, 2013), http://bit.ly/1vvXvXG.

investigative targets and others.[26] Troublingly, although a number of court-ordered rules restrict the NSA's ability to use and access information obtained under the call-records program, the government violated those rules for years.[27]

The government routinely relies on its call-records database in criminal investigations like this one.[28] For example, the government is permitted to freely query its phone-records database using the phone numbers of individuals for whom it has obtained a FISA warrant—like Mr. Muhtorov and Mr. Jumaev here.[29] Those call-records queries allow investigators to probe a suspect's telephone contacts. In this case, the government has pointed to hundreds of phone calls made or received by the defendants. *See* Section I. Some of the phone calls between Mr. Muhtorov and Mr. Jumaev—or between the defendants and others—may initially have been identified using precisely this program. Moreover, the government may have relied, in part, on phone records the NSA collected in 2009, when it was still violating the court-ordered rules that restricted its collection, use, and dissemination of this sensitive information. *See* Section I (discussing communications between the defendants in 2009).

---

[26] *See* Primary Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 14-96 (FISC June 19, 2014), http://1.usa.gov/1oLUFtg.

[27] *See, e.g.*, Order at 8–9, *In re Prod. of Tangible Things From [Redacted]*, No. BR 08-13 (FISC Mar. 2, 2009), http://bit.ly/1rJup07 (finding that the government's "failure to ensure that responsible officials adequately understood the NSA's alert process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations").

[28] *See, e.g.*, *id.* at 13 (describing 2,549 telephone numbers that the NSA tipped to the FBI, and the FBI's investigation of U.S. persons based on such tips).

[29] *See, e.g.*, Primary Order 8–9, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 11-07 (FISC Jan. 20, 2011), http://1.usa.gov/1tyykiI (approving for querying "[i]dentifiers that are currently the subject of electronic surveillance" authorized by the FISC).

The NSA's call-records program has been deemed unconstitutional by one court because it violates the Fourth Amendment,[30] yet the government has never provided official notice of this surveillance to a single criminal defendant. Only one defendant has ever learned that the program was used in his case—*United States v. Moalin*, No. 10-CR-4246 (S.D. Cal.)—and he only discovered that fact *after* his trial was over, when government officials sought to justify the bulk call-records program by pointing to his case in congressional testimony.[31] In short, the government appears to believe that it has no legal obligation to tell criminal defendants when it relies on evidence derived from the NSA's bulk collection of call records.

C. The NSA Internet-Metadata Program

The government's investigations of Mr. Muhtorov and Mr. Jumaev may well have relied on yet another bulk-collection program: the NSA's internet-metadata program. From 2001 to 2011, the NSA tracked the online activities of Americans by collecting internet metadata in bulk. (The program is sometimes known as the NSA's "PR/TT" program because, beginning in 2004, it was operated on the basis of FISA's pen register/trap-and-trace provisions, 50 U.S.C. §§ 1841–1846.) Under this program, the government acquired multiple types of internet records, including information about the senders and recipients of email messages and records of internet activity.[32] Once

---

[30] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013). *But see ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (appeal pending).

[31] *See, e.g.*, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Committee on Intelligence*, 113th Cong. (June 18, 2013), http://1.usa.gov/1mz0YjI (statement of FBI Deputy Director Sean Joyce).

[32] For instance, the government may have also collected information about internet transactions such as logging into or out of a web-based account, or the processing of an instant message communication. *See* Memorandum Opinion at 34–35, *[Redacted]*, No.

collected, the internet records were stored in a government database for several years, where the NSA queried those records to search for connections between its targets and others—much as it does using the call-records program discussed above.

The FBI, DOJ, and other agencies used information derived from the internet-metadata program in the course of investigations for years—including the period covered by the government's investigation in this case.[33] At one point, the NSA estimated that hundreds of accounts would be "tipped" to the FBI and CIA each year under the program, and that approximately 25 percent of those accounts would be associated with U.S. persons.[34] The Foreign Intelligence Surveillance Court ("FISC") imposed a number of restrictions on the NSA's ability to disseminate information obtained under this program—yet, from 2004 through at least 2009, the government repeatedly violated those court-ordered restrictions.[35]

Indeed, for years, the NSA failed to abide by the FISC's rules for collecting, querying, and handling internet metadata.[36] From the outset of the PR/TT program, the NSA continuously and systematically over-collected Americans' internet records in

---

PR/TT [Redacted] (FISC [Redacted]) (Bates, J.), http://1.usa.gov/1q3af5P ("FISC 2010 Op.").

[33] *See, e.g.*, Decl. of Lt. Gen. Keith B. Alexander at 16 n.7, No. PR/TT [Redacted] (FISC [Redacted]), http://bit.ly/1r4t72o (describing the NSA's provision of "research to Department of Justice or Department of Defense personnel for their review in connection with criminal or detainee proceedings").

[34] *See* Opinion & Order at 46, *[Redacted]*, No. PR/TT [Redacted] (FISC [Redacted]) (Kollar-Kotelly, J.), http://1.usa.gov/1lPEe07 ("FISC 2004 Op.").

[35] FISC 2010 Op. at 12, 17–22; FISC 2004 Op. at 80–87.

[36] FISC 2010 Op. at 9–22 (describing the NSA's "substantial non-compliance" and "systemic overcollection" of metadata); Order at 6–7, *[Redacted]*, No. PR/TT [Redacted] & *In re Application of the FBI for an Order Requiring the Production of Tangible Things From [Redacted]*, No. BR 09-06 (FISC June 22, 2009), http://1.usa.gov/1tioe5f.

violation of the FISC's orders, which had authorized the collection of only specified categories of metadata. According to the government, for several years, "virtually every PR/TT record" generated by the program contained some illegally collected data.[37] Although the FISC acknowledged these violations in 2010, it did not require the government to identify and destroy all of the illegally acquired information. Instead, it allowed the government to retain and search this data so long as it claimed not to know whether the information was acquired through unauthorized electronic surveillance.[38] In December 2011, the government reportedly decided not to seek reauthorization of the internet-metadata program for operational reasons.[39]

As discussed above, the government relies on intercepted email communications as well as records of Mr. Muhtorov's and Mr. Jumaev's other internet activities—activities that may have first been tracked through the bulk collection of the defendants' internet metadata. *See* Section I. Because the government's investigation was active in 2011—and, in all likelihood, in 2010—it likely relied on information collected during precisely the period when the NSA operated the PR/TT program in violation of court-ordered rules.

Even beyond these compliance violations, the NSA's internet-metadata program raises constitutional and statutory questions on par with the NSA's call-records program. *Cf.* Compl., *First Unitarian Church of L.A. v. NSA*, No. 13-cv-3287 (N.D. Cal. July 16,

---

[37] FISC 2010 Op. at 20–21; NSA Response to FISA Court Questions at 18, Letter from David S. Kris, Asst. Att'y Gen., to the Hon. John D. Bates, Presiding Judge, U.S. FISC, [Date Redacted], http://1.usa.gov/Ze0Ugi.

[38] FISC 2010 Op. at 114-15.

[39] Unclassified Declaration of Teresa H. Shea at 15, *Jewel v. NSA*, 08-cv-4373-JSW (N.D. Cal. Mar. 19, 2014) (ECF No. 228), http://bit.ly/1lLZPGr.

2013) (asserting statutory, Fourth Amendment, and First Amendment challenges to the NSA's bulk collection of telephony metadata). Although FISA expressly requires notice of this surveillance, *see* 50 U.S.C. 1845(c), the government has never provided notice of the NSA's internet-metadata program to a single criminal defendant.

D. Bulk Collection of Financial Records

There is evidence also that the government collects financial records in bulk—including international money transfers like those the government monitored in this investigation. In November 2013, *The New York Times* and *The Wall Street Journal* reported that the Central Intelligence Agency ("CIA") was collecting records of these transfers in bulk from companies like Western Union and MoneyGram.[40] The financial records program is reportedly conducted under Section 215, 50 U.S.C. § 1861. The CIA has used the information it collects in bulk to amass "a vast database of international money transfers that includes millions of Americans' financial and personal data," including Social Security numbers.[41] The data is analyzed by the CIA and then shared with other agencies like the FBI. According to a former official, "[I]f a CIA analyst searches the data and discovers possible suspicious terrorist activity in the U.S., the analyst provides that information to the FBI."[42] No criminal defendant, however, has ever received notice of the government's reliance on this bulk collection program.

[40] Charlie Savage & Mark Mazzetti, *C.I.A. Collects Global Data on Transfers of Money*, N.Y. Times, Nov. 13, 2013, http://nyti.ms/1lbhseL; Siobhan Gorman, Devlin Barrett & Jennifer Valentino-DeVries, *CIA's Financial Spying Bags Data on Americans*, Wall St. J., Jan. 25, 2014, http://on.wsj.com/1dO2n2T.

[41] *Id.*

[42] *Id.*

It is plain that the government monitored international money transfers by the defendants in this case, including Western Union and MoneyGram transactions. *See* Section I (describing Mr. Muhtorov's use of these international monetary services since at least 2007 and Mr. Jumaev's use of them between 2000 and 2012). The FBI claims that it obtained evidence of one such transfer by searching Mr. Jumaev's trash, *see* Bates No. G_000303, but that may be one instance of the "parallel construction" that law-enforcement agencies reportedly use to conceal tips and leads they receive from intelligence agencies.[43] Mr. Muhtorov and Mr. Jumaev are entitled to notice if the government's investigation relied on the bulk collection of their financial records.

E. Other Surveillance Techniques

Given the number of surveillance programs the government concealed for years, it is possible that the government relied on other, still-secret surveillance techniques in its investigations of Mr. Muhtorov and Mr. Jumaev. Disclosures suggest that it may have tracked the defendants' locations, other financial activities, or various other kinds of communications data. Defendants' motion to compel notice is not limited to the surveillance programs described above or surveillance methods the government has publicly acknowledged to date.[44] Rather, it encompasses any surveillance program or technique that the government used to monitor the defendants' communications or activities as part of its investigation.

---

[43] *See* John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/1h07Hkl (describing DEA's use of "parallel construction" to conceal its reliance on information derived from NSA surveillance).

[44] *See* Charlie Savage & Mark Mazzetti, *C.I.A. Collects Global Data on Transfers of Money*, N.Y. Times, Nov. 13, 2013, http://nyti.ms/1lbhseL ("Several officials also said more than one other bulk collection program has yet to come to light.").

IV. The Defendants Are Entitled to Notice

A. Due Process Entitles the Defendants to Notice

Mr. Muhtorov and Mr. Jumaev are entitled to notice of the surveillance techniques that contributed to the government's investigation, so that they may challenge the legality of the surveillance and the admissibility of the resulting evidence. The government cannot preempt the right to seek suppression by withholding notice based on its own conclusion that its methods were lawful. Rather, the defendants are entitled to have the *Court*—not the government—decide issues going to their basic constitutional rights. Those questions include (1) whether the government's surveillance violated the Fourth Amendment or other legal protections, and (2) whether the government's evidence is in fact "derived" from such surveillance. *See, e.g.*, *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972); *Alderman v. United States*, 394 U.S. 165 (1969).

The only way to effectuate a criminal defendant's right to suppress illegally acquired evidence is through notice. This suppression right becomes especially important when the government adopts new and intrusive surveillance techniques. By now, it is clear that the government routinely employs legally untested surveillance methods in aid of investigations like this one—and that it often seeks to conceal those methods in order to avoid court review.[45] But due process rights grounded in the Fourth and Fifth Amendments entitle the defendants to challenge the legality of these surveillance

[45] *See* Savage 12,333 Article (describing continuing efforts to avoid giving notice of E.O. 12,333 surveillance); Savage FAA Article (describing five-year effort to avoid giving notice of FAA surveillance); John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/1h07Hkl (describing use of "parallel construction" to conceal reliance on information obtained from intelligence agencies).

techniques and to seek suppression of the resulting evidence. *See 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 right to seek suppression of evidence "derived" from an unlawful search).[46]

The exercise of the suppression right depends entirely on notice. Thus, courts have long found notice a constitutionally required element of surreptitious searches like wiretaps and sneak-and-peak entries. *See Berger v. New York*, 388 U.S. 41, 60 (1967) (finding wiretapping statute unconstitutional because, among other things, it had "no requirement for notice as do conventional warrants"); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peak warrant constitutionally defective for its failure to provide explicitly for notice within a reasonable time); *United States v. Dalia*, 441 U.S. 238, 247–48 (1979) (observing that Title III provided "a *constitutionally adequate substitute for advance notice* by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance" (emphasis added)).

[46] The defendants' right to notice is also found within the government's *Brady* obligation. In order to comply with that requirement, the government must disclose any information material to a defendant's motion to suppress evidence. *See United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000); *Smith v. Black*, 904 F.2d 950, 965–66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992) (due process mandates the disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression hearing"). It goes without saying that in order to seek suppression, the defendants must be aware of the surveillance that served as the source(s) of the government's evidence. As a result, *Brady* requires the government to give notice of the surveillance techniques used to monitor the communications or activities of the defendants that were relied upon in the investigation, and the information obtained or derived from that surveillance.

Congress has responded to these rulings by incorporating express notice provisions into many surveillance statutes. *See, e.g.*, 18 U.S.C. § 2518(8)(d) (Title III); S. Rep. No. 1097, at 2194 (1968) (explaining the inclusion of a notice requirement in Title III's wiretapping provisions, and citing *Berger*); *see also* 50 U.S.C. § 1806(c) (FISA electronic surveillance); *id.* § 1825(d) (FISA physical search); *id*. § 1842(c) (FISA pen register); *cf.* Fed. R. Crim. P. 41(f) (requiring notice).

As the cases above show, today is not the first time courts have had to confront the government's use of new technologies to carry out surreptitious searches. The use of secret wiretapping and electronic recording devices in criminal investigations posed similarly novel legal problems in the last century. The courts that addressed the legality of these methods—and laid down the rules governing their use—were only able to do so because the defendants received notice of that surveillance. Thus, in *Keith*, the government responded to the defendant's motion to compel the disclosure of electronic surveillance information in a national-security prosecution by publicly acknowledging that investigators had overheard the defendant's conversations using wiretaps. 407 U.S. at 299–300. In *Kyllo*, the defendant had notice that the government's search warrant application relied on evidence gathered using thermal-imaging technology. *Kyllo v. United States*, 533 U.S. 27, 29–30 (2001). Likewise, in *Jones*, the defendant had notice of the government's use of GPS tracking in order to record his movements. *United States v. Jones*, 132 S. Ct. 945, 948 (2011). All of these seminal Fourth Amendment decisions would have been impossible if the defendants had not received notice of the government's secret searches.

Equally here, the Court must ensure that the defendants have sufficient notice of any surveillance of their communications or activities to allow them to press their claims fairly before the Court. For the reasons described above, it appears extremely unlikely that the government has applied such a standard in making its notice determinations in this case. For instance, the government apparently believes that it has no obligation to give notice *any time* its evidence is derived from E.O. 12,333 surveillance. *See* Savage 12,333 Article (describing the government's view that "defendants have no right to know" if investigators derived evidence from an E.O. 12,333 intercept). Similarly, the government appears to believe that it has no obligation to provide notice when it relies on the NSA's bulk collection of call records in criminal investigations, *see* Section III.B—perhaps because it does not believe its collection and querying of these records constitutes a "search." But the call-records program plainly presents novel questions of a constitutional dimension, and one court has already found the program unlawful. *See Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013). It is not the government's prerogative to secretly and self-servingly conclude that its surveillance is legal and then to withhold notice from criminal defendants on that basis.

This point is a commonsense one. Due process entitles the defendants to test, on the facts of this case, whether the government's evidence should be suppressed as the fruit of unlawful surveillance. Due process does not leave these questions to the government's sole judgment and discretion. *See Alderman v. United States*, 394 U.S. 165, 168 (1969) (recounting, in wiretapping challenge, Supreme Court's refusal "to accept the *ex parte* determination of relevance by the Department of Justice in lieu of adversary proceedings in the District Court"); *Kolod v. United States*, 390 U.S. 136, 136–37 (1968)

(prior proceedings); *cf., e.g., United States v. Eastman*, 465 F.2d 1057, 1062–63 & n.13 (3d Cir. 1972) (concluding that the Wiretap Act's statutory notice provision was "intended to provide the defendant whose telephone has been subject to wiretap an opportunity to test the validity of the wiretapping authorization"). It would make little sense if the government could pre-determine, as part of its notice analysis, difficult or novel legal questions that a defendant would properly put before the Court—if only he knew.

The government's definition of "derived" evidence is especially opaque and problematic—yet notice in many cases turns on that definition. According to reports, the government has long held a "narrow understanding of what 'derived from' means in terms of when it must disclose specifics to defendants" in the context of foreign-intelligence surveillance. Savage FAA Article. The government has never publicly described that "narrow understanding"—either before or after its notice policies began to draw scrutiny in the past year. But the consequences are significant. If the government is defining "derived" evidence more narrowly than the Constitution allows,[47] and withholding notice on that basis, then it is concealing the underlying sources of its evidence, and thereby insulating them from judicial review. The government's failure to provide notice of FAA surveillance in this case or any other for five years relied on precisely this type of evidence laundering. *See id.* Similarly, when the government engages in parallel construction—in order to conceal the nature of its underlying

[47] *See, e.g., Murray*, 487 U.S. at 536–37 (prohibiting "the introduction of derivative evidence, both tangible and testimonial, that is the product of the [unlawful search], or that is otherwise acquired as an indirect result of the unlawful search, up to the point at which the connection with the unlawful search becomes 'so attenuated as to dissipate the taint'").

investigation—that is a refusal to give notice of "derived" evidence as due process requires.[48]

The Supreme Court has repeatedly made clear that when the government chooses to criminally prosecute an individual, it may not keep secret the sources of its evidence.

> [T]he 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 his defense.

Jencks v. United States, 353 U.S. 657, 670–71 (1957) (quoting *United States v. Reynolds*, 345 U.S. 1, 12 (1953)). Simply put, the government may not have it both ways—its secrecy and its prosecution—when an individual's liberty is at stake. Indeed, due process requires not only notice to a defendant, but may also call for disclosure of underlying surveillance applications or intercepts. In *Keith*, the Supreme Court compelled the government to turn over records of wiretapped conversations in a national-security case, even as the government threatened to abandon the prosecution if required to disclose them. *See* 407 U.S. at 318–24, *aff'g* 444 F.2d 651, 655 (6th Cir. 1971) (discussing the government's assertions). The Court did not blink—it ordered disclosure. *See* 407 U.S. at 324. The government is bound by that same choice here, wherever it has relied on undisclosed surveillance programs in the conduct of its investigation.

Accordingly, the government must give notice of the surveillance techniques that contributed to its investigation of Mr. Muhtorov and Mr. Jumaev—so that the Court may ultimately decide whether there is a legal and factual basis for suppression.

---

[48] *See, e.g.*, John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/1h07Hkl.

B. 18 U.S.C. § 3504 Entitles the Defendants to Notice

Congress has also provided a right to notice of electronic surveillance by statute. Under 18 U.S.C. § 3504(a), 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 defines "unlawful act" as "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." *Id.* § 3504(b).

The government has recognized that 18 U.S.C. § 3504 requires "the affirmance or denial of the *fact* of electronic surveillance, even if the government believes it was lawful." David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions 2d* at § 27:12 (emphasis in original). A "cognizable claim" for notice under the statute "need be no more than a 'mere assertion,' provided that it is a positive statement that illegal surveillance has taken place." *United States v. Apple*, 915 F.2d 899, 905 (4th Cir. 1990) (citing *United States v. Tucker*, 526 F.2d 279, 282 & n.4 (5th Cir. 1976)). The party must make a prima facie showing that he was "aggrieved" by the surveillance—*i.e.*, "that he was a party to an intercepted communication, that the government's efforts were directed at him, or that the intercepted communications took place on his premises." *Apple*, 915 F.2d at 905. Because a defendant will have only limited information about the government's undisclosed surveillance, this initial showing need not be complete; it must only have a "colorable basis." *Id.* (citing *United States v. Pacella*, 622 F.2d 640, 643 (2d Cir. 1980)).

Mr. Muhtorov and Mr. Jumaev have made such a showing. The government has described or disclosed numerous communications involving the defendants while refusing to specify how it obtained them. *See* Section I. Those include the defendants' international communications and their online activities, which could readily have been vacuumed up by the government's dragnet collection of content and metadata under Executive Order 12,333. *See* Section III.A. Separately, the government has acknowledged the *domestic* collection of internet metadata in bulk for at least ten years, up until 2011, under the NSA's PR/TT program. *See* Section III.C. That program involved the interception of defendants' metadata and/or communications, and was directed at defendants (as well as many others), rendering them aggrieved under section 3504. *See generally United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1991) ("[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at that time."). Finally, the government has acknowledged the NSA's bulk collection of phone records over a period of years that spans its investigation in this case. Through that program, the NSA obtained the call records of millions of individuals across multiple phone companies, and it uses that aggregated data to track the calls of individuals who are the subject of foreign-intelligence surveillance, like the defendants here. *See* Section III.B.

Accordingly, the government must provide notice of the surveillance methods used in this case and its purported legal authorities. *See United States v. Alter*, 482 F.2d 1016, 1027 (9th Cir. 1973) (holding that the government's response to a claim under section 3504 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).

C. 50 U.S.C. § 1845 Entitles the Defendants to Notice

Finally, FISA expressly requires notice of surveillance conducted pursuant to the statute's pen-register and trap-and-trace provisions. 50 U.S.C. § 1845(c). The NSA's internet-metadata program was, for seven years, conducted under this authority. If the government used data obtained via this program in its investigation of the defendants, it must give notice so that they may seek to suppress any resulting evidence.

CONCLUSION

For the reasons above, Mr. Muhtorov and Mr. Jumaev respectfully request that the Court issue an order compelling the government to provide notice of: (1) each surveillance technique it used to obtain information about the defendants' communications or activities in its investigation; (2) the timing or duration of that surveillance; (3) the legal authority relied upon; and (4) the evidence obtained or derived from that surveillance.

Dated this 20th day of October 2014.

Respectfully submitted,

VIRGINIA L. GRADY
Federal Public Defender

/s/ Warren R. Williamson
WARREN R. WILLIAMSON
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, Colorado 80202
Telephone: (303) 294-7002
Fax: (303) 294-1192
Rick.Williamson@fd.org

/s/Brian Rowland Leedy
Brian Rowland Leedy
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, CO 80202
Telephone: (303) 294-7002
Fax: (303) 294-1192
Brian_Leedy@fd.org

/s/ Kathryn J. Stimson
Kathryn J. Stimson,
Attorney at Law
1544 Race Street
Denver, CO 80206
Telephone: (720) 638-1487
kathryn@stimsondefense.com

/s/ Patrick C. Toomey
Patrick C. Toomey
American Civil Liberties Union Foundation
125 Broad St., 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
ptoomey@aclu.org

Attorneys for Jamshid Muhtorov

/s/ David Barry Savitz
David Barry Savitz
Law Office of David B. Savitz
1512 Larimer Street, Suite 600
Denver, CO 80202
Telephone: (303) 825-3109
savmater@aol.com

/s/ Mitchell Baker
Mitch Baker, Attorney at Law
1543 Champa Street, #400
Denver, CO 80202
Telephone: (303) 592-7353
mitchbaker@estreet.com

Attorneys for Bakhtiyor Jumaev

On the brief:

Jameel Jaffer
Alex Abdo
Ashley Gorski
Attorneys at Law
American Civil Liberties Union Foundation
125 Broad St., 18th Floor
New York, NY 10004
Telephone: (212) 519-7816
Fax: (212) 549-2654
jjaffer@aclu.org

Mark Silverstein
Sara J. Rich
Attorneys at Law
ACLU Foundation of Colorado
303 E. 17th Avenue, Suite 350
Denver, Colorado 80203
Phone: (303) 777-5482;
Fax: (303) 777-1773
msilverstein@aclu-co.org

CERTIFICATE OF SERVICE

I hereby certify that on October 20, 2014, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following email address:

Gregory A. Holloway
Assistant U.S. Attorney
Email: gregory.holloway@usdoj.gov

Erin Martha Creegan
National Security Division for the U.S. Dept. of Justice
Email: erin.creegan@usdoj.gov

I hereby certify that I have mailed or served the document or paper to the following non CM/ECF participant in the manner (mail, hand-delivery, etc.) indicated by the non-participant's name:

Mr. Jamshid Muhtorov *(Via U.S. Mail)*

Mr. Bakhtiyor Jumaev *(Via U.S. Mail)*

/s/ Warren R. Williamson
WARREN R. WILLIAMSON
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, Colorado 80202
Telephone: (303) 294-7002
Fax: (303) 294-1192
Rick.Williamson@fd.org

Attorney for Defendant Jamshid Muhtorov