IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. BAKHTIYOR JUMAEV,

Defendant.

DEFENDANT JUMAEV'S MOTION REQUIRING THE GOVERNMENT TO PROVIDE NOTICE OF INTERCEPTIONS AND/OR SURVEILLANCE OF HIS DEFENSE COUNSEL AND MEMBERS OF HIS DEFENSE TEAM

TABLE OF CONTENTS

I. RELIEF REQUESTED 1

II. INTRODUCTION 2

III. OVERVIEW OF THE FORMS OF SURVEILLANCE AND DATA COLLECTION AT ISSUE 4

A. Section 215 (50 U.S.C. § 1861) 4
B. Executive Order 12333 7
C. FISA and FAA 10

IV. THE GOVERNMENT HAS COLLECTED IMPORTANT INFORMATION FROM TELEPHONE COMMUNICATIONS BY MEMBERS OF THE DEFENSE TEAM AND IT IS REASONABLE TO BELIEVE THAT DEFENSE TEAM COMMUNICATIONS HAVE BEEN, AND ARE BEING, INTERCEPTED 10

A. Section 215 10
B. Executive Order 12333 12
C. FISA and FAA 13

V. DEFENSE TEAM MEMBERS WILL NOT BE ADVISED BY THE GOVERNMENT THAT IT HAS INTERCEPTED THEIR COMMUNICATIONS AND METADATA WITHOUT AN ORDER FROM THIS COURT REQUIRING SUCH NOTICE. 20

A. Section 215 20
B. Executive Order 12333 20
C. FISA and the FAA 21

VI. NOTICE IS NECESSARY TO ENSURE THAT MR. JUMAEV IS AFFORDED HIS SIXTH AMENDMENT RIGHTS AND TO ENSURE THAT THE FOURTH AND SIXTH AMENDMENT RIGHTS OF MEMBERS OF THE DEFENSE TEAM ARE PROTECTED 24

A. Sixth Amendment Concerns 25
B. Fourth Amendment Concerns 28
1. Section 215 28
2. Executive Order 12333 31
3. FISA and FAA 32

VII. CONCLUSION 32

Defendant, Bakhtiyor Jumaev, by and through his counsel, moves this Court for an order requiring the government to provide notice whether communications of his counsel and/or other members of his defense team have been intercepted or otherwise subjected to any type of surveillance since the commencement of each such individual's involvement in the defense of Mr. Jumaev.

I. RELIEF REQUESTED

This motion addresses the collection by the government of the content of any communications, telephone metadata, and any other electronic or physical surveillance of Mr. Jumaev's counsel and the other members of his defense team (collectively "the Defense"). First, the Defense moves this Court to order the government to provide them notice if any such collection and/or interception has occurred. Second, in addition to providing notice of whether such interception, surveillance, or collection of information has occurred, the Defense moves for an order requiring the government to describe what communications, metadata and other information have been collected, intercepted or surveilled and the periods of time of such collection, interception, or surveillance. Third, the Defense moves the Court to require the government to set forth with specificity the procedures employed by the government to determine whether counsel or other members of the defense team have been surveilled and whether their actual communications and/or metadata have been collected. Finally, the Defense moves the Court to order the government to set forth the minimization procedures used with respect to any communications or data collected; and to identify the existence of a filter

team and filter team protocols that have been used or are currently being used by the government in this case. These requests are based on Mr. Juamev's rights to counsel, a fair trial, present a defense, and fundamental due process. The requests are also based on counsel's right to be free from unreasonable searches and seizures. U.S. Const. Am. IV.

II. INTRODUCTION

In this case, the Defense has extensively researched factual and legal issues concerning government surveillance of Mr. Jumaev. In conducting this research on behalf of Mr. Jumaev, the pervasive nature and scope of our government's surveillance and spying has been a stunning revelation. The government routinely spies on governmental leaders of our allies,[1] and has admitted spying on members of the United States Congress.[2] At least one federal judge has characterized our government's spying technology as "almost Orwellian." *Klayman* v. *Obama*, 957 F. Supp. 2d 1, 33 (D.D.C. 2013).

Particularly germane to the issue before this Court is the breadth and magnitude of surveillance and the collection of massive amounts of information on American citizens and persons located on our soil. The startling reality is that

[1] *See* James Ball, NSA Monitored Calls Of 35 World Leaders After US Official Handed Over Contacts, The Guardian, October 24, 2013, *available at* http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

[2] *See* Greg Miller, *CIA Director John Brennan Apologizes For Search Of Senate Committee's Computers*, Washington Post, July 31, 2014, *available at http://www.washingtonpost.com/...of-senate-computers/2014/07/31/28004b18-18c6-11e4-9349-84d4a85be981_story.html?wpisrc=al_national%5B7/31/2014 7:14:45 PM%5D).*

anyone who uses a cell phone or the Internet in this country is likely to have been subjected to such surveillance.

This motion describes several forms of surveillance and mass information collection used by our government that may or may not be authorized by various United States laws. The motion will further set forth facts establishing that our government has collected confidential information from telephone communications by members of the Defense. Finally, the motion will set forth facts showing why it is reasonable to believe that communications between members of the Defense have been and continue to be intercepted.

The motion describes notice provisions, if any, provided by each of the relevant laws, and the government's position interpreting any notice requirement as it applies to each form of surveillance discussed herein. Neither the laws under which the collection of information and surveillance are ostensibly authorized, nor the government's previous positions set forth on the record when Mr. Jumaev has requested notice in related matters, provide for any form of notice of surveillance to the Defense. Hence, the need for this Court's intervention.

Previous filings in this case have demonstrated that the surveillance and collection of information by the government violate Mr. Jumaev's rights under the United States Constitution. These actions by the government also implicate the Defense team's rights under the Fourth and Sixth Amendments.

III. OVERVIEW OF THE FORMS OF SURVEILLANCE AND DATA COLLECTION AT ISSUE

A. Section 215 (50 U.S.C. § 1861)

Section 215 of the Patriot Act (50 U.S.C. § 1861) allows the government to obtain secret court orders from the FISC and to compel third parties to produce "any tangible thing" that is "relevant" to foreign intelligence or terrorism investigations. Telephone metadata is included in the government's interpretation of "tangible things." Since May of 2006, at least 36 orders requiring United States telecommunication providers to turn over bulk telephone metadata to the FBI and NSA have been issued by FISC judges. The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World, December 12, 2013*, at 94 (the "*President's Review*").[3]

> What this means, in effect, is that specified service providers must turn over to the government on an ongoing basis call records for every telephone call made in, to, or from the United States through their respective systems. NSA retains the bulk telephony meta-data for a period of five years.

Id., at 97.[4]

Metadata is the information attached to phone calls and emails, *i.e*., " data that provides information about other data." *Merriam-Webster Online Dictionary*, *available at* http://www.merriam-webster.com/dictionary/metadata. Metadata swept up by the government from telephone service providers can contain

[3] The *President's Review* is available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[4] As the *President's Review* notes at 203, whether the collection of bulk telephone metadata is actually authorized by Section 215, "posed serious and difficult questions of statutory and constitutional interpretation about which reasonable lawyers and judges could certainly differ."

information about the date and time of the communication, the phone numbers of the caller and the receiver, their respective geographic locations and the amount of data transmitted.[5] In practical terms, telephone metadata is capable of revealing an enormous amount of personal, private and confidential information. *President's Review*, at 117 concluded that the types of private information revealed by GPS monitoring addressed in *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012) are functionally similar to information obtained by telephone metadata collection. Quoting Justice Sotamayor's observations in *Jone*s, the Commission found that metadata can reveal:

> "a wealth of detail" about an individual's "familial, political, professional, religious, and sexual associations." It can reveal calls "to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar, and on and on."

---

[5] The orders that have been made public do not provide for location information to be turned over to the government. However, Senators Udall, Wydens, and Heinrich, all members of the Senate Select Committee on Intelligence filed an *Amicus* brief in Clapper v. Amnesty Int'l USA, ___U.S. ___, 133 S. Ct. 1138,185 L. Ed. 2d 264, 2013) in which they assert information obtained through FOIA revealed that the executive branch has interpreted its authority under Section 215 to allow the collection of information about Americans' locations. Brief for Former members of the Church Committee and Law Professors, at 23--25, No. 11-1025, 2012 U.S. S. Ct. Briefs LEXIS 4001, at *30-41 (2012); *see also Letter from [Redacted], Attorney, Office of General Counsel, NSA, to SSCI*, (Apr. 1, 2011), at 1, *available at* http://www.dni.gov/files/documents/501/NSA CSLI Gottsman Response_SealedFINAL.pdf. And FISC opinions continue to refer to still-undisclosed "secret law " interpreting crucial statutory terms in FISA related to bulk collection as well as addressing the compatibility of bulk collection with the Fourth Amendment. *See In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED],* Case No. BR 13-109, 2013 WL 5741573, at *6, 2013 U.S. Dist. LEXIS 134786, at *29 (F.I.S.C., Aug. 29, 2013) (released in redacted form Sept. 17, 2013). (FISC "has previously examined the issue of relevance for bulk collections."

President's Review, at 117 (quoting *Jones* at 132 S. Ct. at 945, 181 L. Ed.2d at 15 925) (Sotomayor, J. concurring; footnote omitted).[6]

In addition to the detailed personal information described above, the collection of metadata raises additional concerns in the context of an attorney's work and that of members of the defense team. By way of example and not by limitation, metadata can reveal to the government what witnesses and experts have been contacted by the Defense, which of those persons have contacted the Defense, the date, time, and duration of each contact, the frequency of such contacts, etc. and by negative inference, what witnesses or individuals the Defense may not have located or identified as significant.

Once stored, the metadata is subsequently searched or queried by the government. In a case such as Mr. Jumaev's, an NSA analyst will use an identifier associated with terrorism, referred to as a "seed number," to generate a list of all telephone numbers in contact with the seed number over the preceding five years. This is referred to as the first "hop". A second query is then conducted. For example, if 100 phone numbers have been in contact with the number in question over a five-year period, and in turn each of those numbers has been in contact with 100 numbers over that five-year period, then ten thousand numbers will be evaluated (100x100).

---

[6] *See also* Clifton B. Parker, *Stanford Students Show That Phone Record Surveillance Can Yield Vast Amounts Of Information*, Stanford News, (March 12, 2014), *available at* http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html (researchers showed how medical, financial and other personal information could be disclosed just by cross-referencing phone metadata with publicly available databases).

Based upon the government's description of how section 215 data is queried, the court in *Klayman* v. *Obama* determined that everyone has been searched, or "analyzed", either manually or automatically. 957 F. Supp. 2d at 36-37. The *President's Review* recognized that, irrespective of whether a search has actually occurred, knowledge that "the government is one flick of a switch" away from the wealth of information contained in its mass of stored metadata can have a profound chilling effect on associative and expressive freedoms. *President's Review*, at 117. The government's collection of, and ability to search, the metadata has a chilling effect on the manner in which attorneys defending clients charged with terrorism offenses are able to communicate between themselves and with others.

B. Executive Order 12333

Executive Order No. 12333, 46 FR 59941 (Dec. 4,1981), (hereinafter "EO 12333") was originally enacted by President Reagan in 1981 and "establishes the framework in which our governmental and military agencies are to effectuate the process of gathering foreign intelligence and counterintelligence information, and the manner in which intelligence-gathering functions will be conducted at home and abroad." *United Presbyterian Church v. Reagan*, 557 F. Supp. 61, 62 (D.C. 1982). Unlike Section 215, EO 12333 allows for collection of the actual content of communications of U.S. persons, in addition to metadata. In short, surveillance is conducted without judicial oversight and with comparatively little Congressional review. Despite this tool's existence for over thirteen years, no case law exists evaluating its constitutionality.

EO12333 was not intended to apply to domestic communications. Changes in the way electronic information is stored and transmitted have eliminated the protections originally intended to render EO 12333 inapplicable to domestic communications. John Napier Tye, former Department of State official described the program and his concerns in a recent Op-Ed. piece in the Washington Post.[7] As Tye stressed:

> [T]oday, U.S. communications increasingly travel across U.S. borders — or are stored beyond them. For example, the Google and Yahoo e-mail systems rely on networks of "mirror" servers located throughout the world. An e-mail from New York to New Jersey is likely to wind up on servers in Brazil, Japan and Britain. The same is true for most purely domestic communications.

As Tye further pointed out, surveillance abroad requires a warrant when the target is a U.S. person but, if collection is coming from a data center overseas, large volumes of Americans' communications may be picked up as "incidental" to collection on a foreign target:

> Unlike Section 215, the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons be suspected of wrongdoing and places no limits on the volume of communications by U.S. persons that may be collected and retained.

---

[7] *See* James Napier Tye, *The Reagan Rule That Lets The NSA Spy On Americans*, Washington Post, July 18, 2014, *available at* http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

Id. Tye implied that the government was continuing to gather email metadata under EO12333.[8] Tye warned that Section 215 may only be a "mechanism to backfill that portion of U.S. person data that cannot be collected overseas under 12333." *Id.*

In its brief submitted to the Supreme Court in *Clapper v. Amnesty Int'l USA*, ___ U.S. ___, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013), the government argued "that it can conduct FISA-exempt human and technical surveillance programs that are governed by Executive Order 12333". 133 S. Ct. at 1149, 185 L. Ed. 2d at 278.[9] In the March 2014 Privacy and Civil Liberties Oversight Board (hereafter PCLOB) [10] hearings on the FAA, Robert Litt, General Counsel, Office of the Director of National Intelligence, stated:

> Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated. There is a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons.[11]

---

[8] Former NSA Director General Keith Alexander stated publicly that the email metadata program authorized by the Patriot Act was terminated in 2011. He did not state that the NSA had stopped collecting such data.

[9] The *Clapper* Court noted that it did not reach the issue of whether EO 12333 existed as an alternative to FAA for collection of such information. 133 S. Ct. at 1149, 185 L.Ed at 278.

[10] According to its, website http://www.pclob.gov, "[t]he PCLOB is an independent agency within the executive branch established by the Implementing Recommendations of the 9/11 Commission Act of 2007.

[11] *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, transcript at 81 (March 19, 2014), *available at* http://www.pclob.gov/Library/20140319-Transcript.pdf. The categories of personal information are listed in EO 12333, part 2(a)-(j) and includes "collection, retention and dissemination" of "[i]nformation concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility";

EO 12333 therefore is capable of being the basis of surveillance of the Defense both intentionally and "inadvertently'.

C. FISA and FAA

Messrs. Jumaev and Muhtorov have filed several pleadings detailing the provisions of FISA (50 U.S.C. §§ 1801-1811, 1821-1829), and the 2008 amendments to FISA and FAA.[12] These pleadings have familiarized the Court with the provisions of FISA and the bulk collections of communications occurring under the purported authority of the FAA. The prior pleadings describe the scope and manner of surveillance and information gathering accomplished by the government pursuant to its claims of authority under FISA and the FAA and are incorporated herein by reference.

IV. THE GOVERNMENT HAS COLLECTED IMPORTANT INFORMATION FROM TELEPHONE COMMUNICATIONS BY MEMBERS OF THE DEFENSE TEAM AND IT IS REASONABLE TO BELIEVE THAT DEFENSE TEAM COMMUNICATIONS HAVE BEEN, AND ARE BEING, INTERCEPTED

A. Section 215

It is beyond dispute that the metadata associated with the phones of members of the Defense has been collected and analyzed. The "government "has declassified and authenticated an April 25, 2013 FISC Order signed by Judge Vinson, which confirms that the NSA has indeed collected telephony

---

"[i]nformation arising out of a lawful personnel, physical or communications security investigation"; "[i]nformation acquired by overhead reconnaissance not directed at specific United States persons"; and "[i]ncidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws. *See id.* Part 2(f)-(i).

[12] *See* Docs. 14, 125,157, 458, 499, 520, 521, 578, 584, 590, 602, 603, and 617.

metadata from Verizon." *Klayman v. Obama*, 957 F. Supp. 2d at 26. The Defense, unlike the plaintiffs In *Clapper v. Amnesty Int'l*, whom a divided Court found to lack standing to challenge FAA's constitutionality, do not have to ask the Court to speculate as to whether they have been surveilled.

> Thus, whereas the plaintiffs in *Clapper* could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention.

Klayman, 957 F. Supp. 2d at 27. Members of the Defense use Verizon and other providers for their telephone usage. Affidavits from current and former members of the Defense are attached as Exhibits A - D, attesting to this usage.

Further, despite the government's argument to the contrary, the district court in *Klayman* found that the government acquisition of metadata was not limited to Verizon customers:

> Put simply, the Government wants it both ways. Virtually all of the Government's briefs and arguments to this Court explain how the Government has acted in good faith to create a comprehensive metadata database that serves as a potentially valuable tool in combating terrorism—in which case, the NSA must have collected metadata from Verizon Wireless, the single largest wireless carrier in the United States, as well as AT&T and Sprint, the second and third-largest carriers.

Id. See also President's Review, at *95* ("The FISC authorized the collection of bulk telephony meta-data under section 215 in reliance "on the assertion of the [NSA] that having access to ***all*** the call records 'is vital to NSA's counterterrorism intelligence'" (quoting *In re Production of Tangible Things from [Undisclosed Service Provider]*, Docket Number: BR-08-13 (FISC Dec. 12, 2008); emphasis

supplied). Judge Leon also concluded in *Klayman* that everyone's metadata is analyzed automatically or manually each time the government runs a query using a "seed" phone number or identifier pertaining to a phone number operating through foreign companies. 957 F. Supp. at 28.

B. Executive Order 12333

Without an order from this Court requiring notice, there simply is no way for the Defense to know if the government is monitoring their confidential and privileged communications. Reliable reports strongly suggest that monitoring has been occurring. As the *President's Review*, at 183, stated:

> [A]ny communication on the Internet might be routed through a location outside of the United States, in which case FISA does not apply and collection is governed under broader authorities such as Executive Order 12333. Today, and unbeknownst to US users, websites and cloud servers may be located outside the United States. Even for a person in the US who never knowingly sends communications abroad, there may be collection by US intelligence agencies outside of the US.

The Defense routinely uses the internet to communicate amongst themselves, communicate with potential witnesses, communicate with experts, and to conduct both legal and fact-based research. Naturally, in the course of handling Mr. Jumaev's defense, terms and/or references, such as "jihad", "Islam", "IJU", "sodiqlar.com", and countless others that are likely of interest to the NSA, are routinely used in these communications and in conducting legal and fact-based research. Reports indicate that the NSA filters communications for words such as those just described to trigger the collection and review of attorney

communications.[13] Virtually everything the Defense does in the course of our attempt to effectively represent Mr. Jumaev in this case renders us a target for government surveillance.

C. FISA and FAA

As will be discussed more fully below, due to the notice provisions set forth in FISA and the FAA, there is no way for the Defense to know if their communications have been, or are being, monitored under either FISA or the FAA. Reliable reports strongly suggest that the government is monitoring our activities and communications.

Collection under the FAA is implicated in several respects. First, the Defense is likely to communicate with non-U.S. persons abroad, a category of communications explicitly authorized to be swept up by the warrantless mass collections that the government justifies under the FAA. "Mass collection" under the FAA means, in numerical terms, that the government collected over one quarter of a billion Internet communications in 2011 alone. *See [Redacted]*, 2011 U.S. Dist. LEXIS 157706, at *102, 2011 WL 10945618, at *10 (FISC Oct. 3, 2011). As described above, terms routinely used by the NSA and other government agencies in searching the mass of collected material would be used

[13] *See, e.g.,* Human Rights Watch *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy, Human Rights Watch,* at 52 (July 28, 2014), *available at* http://www.hrw.org/reports/2014/07/28/liberty-monitor-all. This publication's abstract states:

> The 120-page report documents how national security journalists and lawyers are adopting elaborate steps or otherwise modifying their practices to keep communications, sources, and other confidential information secure in light of revelations of unprecedented US government surveillance of electronic communications and transactions.

during these attorney and defense team communications on behalf of Mr. Jumaev. For that matter, it is likely that merely mentioning Mr. Jumaev's name triggers surveillance since the government has labeled him a terrorist.

Second, defense counsel's international communications will be swept up under the FAA if they merely mention an identified "target". *See 2009* Targeting Procedures 1 (discussing "those cases where NSA seeks to acquire communications about the target that are not to or from the target"); *see also [Redacted]*, 2011 WL 10945618, at *5. As set forth in more detail in Mr. Muhtorov's *Motion to Suppress Evidence Obtained or Derived from Surveillance under the FISA Amendments Act and Motion for Discovery*, at 17-18, (Doc. 520), which is incorporated herein by reference, this surveillance has been detailed in the press and is referred to as "about surveillance." Together with what are referred to as "backdoor searches" this surveillance greatly increases the likelihood that the Jumaev defense team members are being intercepted.

Third, as set forth in detail in Mr. Muhtorov's submission styled *Defendant's Supplemental Authority In Support of His Reply to Government's Response*, at 2-3 (Doc 617) ("*Muhtorov's Supplemental Authority*"), the rationale used by the NSA to judge the "foreignness" of a communication are so broad as to guarantee interception of communications of U.S. persons. The discussion of this issue in Doc. 617 and the attachments thereto are also incorporated by reference. This fact alone greatly increases the likelihood that members of the Defense have been intercepted.

Fourth, incidentally collected material is not discarded but is retained for five years by the government. *President's Review*, at 97. This "incidental" material includes stored conversations of U.S. persons that are then searched by the CIA, FBI, and NSA without a warrant. Again, given the nature of the charges against Mr. Jumaev, there is a great likelihood that search terms applied by the government to this mass of stored data would trigger review of communications collected from members of the Defense.

Fifth, as set forth in detail in *Muhtorov's Supplemental Authority*, at 6, despite that the FAA mass collections are designed by law to avoid collections of communications of U.S. persons, the incidental collections of communications involves a U.S person as often as not. Again, this fact greatly increases the likelihood that members of the Defense have been and continue to be "inadvertently" intercepted. These "inadvertent" interceptions are retained and searched by the government without a warrant.

Finally, it is a virtual certainty that in the process of investigating this case, members of the Defense have contacted and/or researched web sites that the government associates with terrorism. By its very terms, the FAA allows collection of this type of information.

In the context of the Defense's work on behalf of Mr. Jumaev, the government's self-described minimization procedures under the FAA fail to provide meaningful protection. The NSA's recently declassified minimization procedures state as follows:

> Section 4 - Acquisition and Processing - Attorney-Client Communications
>
> As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination.[14]

The procedures expressly contemplate that the NSA will collect attorney-client communications. Moreover, these procedures only apply to post-indictment communications directly between Mr. Jumaev and counsel and are designed to cover only the narrowest reading of attorney client communications under the Sixth Amendment. The minimization procedures, by their very terms, provide absolutely no protection for communications between members of the Defense, communications by defense team members with potential witnesses, and communications by defense team members with potential experts or consultants. In general, these types of communications receive no special protection—they can be acquired, retained, and disseminated like any non-privileged communication.

[14] The NSA's recently declassified minimization procedures are available at https://www.aclu.org/files/natsec/nsa/20130816/FAA Minimization Procedures.pdfsupplemental

FISA itself only states, "No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title [50 USCS §§ 1801 et seq.] shall lose its privileged character." 50 USCS § 1806(a). In Mr. Jumaev's case, and in a number of other reported situations, the government appears to have interpreted the term "privileged communication" in the narrowest possible way, similar to the description of FAA minimization language above. Consequently, communications directly between an unindicted individual and his attorney may be, and have been, intercepted, as noted below. Communications that constitute attorney work product have also been intercepted.

FBI agents interrogated Mr. Jumaev at his Philadelphia apartment on February 14, 2012; at that time, Mr. Jumaev had been charged with an immigration violation, had posted bond that included electronic monitoring, was represented by an immigration attorney, Francois Mazur, Esq., and for approximately two years, unbeknownst to him, had also been under investigation for activities related to this case.[15] The next day, February 15, 2012, Mr. Jumaev called Mr. Mazur and spoke with the attorney's paralegal, seeking legal advice relating to Mr. Jumaev's having been questioned the day prior by the FBI. A copy of the recording of the call, labeled as S2675971321_20120215194017_416.WAV, has been provided in discovery.[16]

[15] The criminal Complaint filed against Mr. Jumaev notes that the FBI had been investigating him in this matter since shortly after his arrest in February 2010 for immigration charges. *See* Doc. 1 at ¶ 13.

[16] Based upon information and belief, to date, the government has not provided all of Mr. Jumaev's intercepted communications. It is therefore currently unknown whether other communications between Mr. Jumaev and his immigration attorney were intercepted.

It is well established that the attorney-client privilege "exists to protect not only the giving of professional advice to those who can act on it, but also the giving of information to the lawyer to enable him to give sound and informed advice." *Upjohn Co. v. United States*, 449 U.S. 383, 390 (1981). Moreover, the privilege extends to paralegals and professional staff who work for an attorney on behalf otf the attorney's client. *See SEPTA v. CaremarkPCS Health, L.P.,* 254 F.R.D. 253, 257 (E.D. Pa. 2008) ("Communications with the subordinate of an attorney, such as a paralegal, are also protected by the attorney-client privilege so long as the subordinate is acting as the agent of a duly qualified attorney under circumstances that would otherwise be sufficient to invoke the privilege.") (internal quotation marks omitted)); *Equity Residential v. Kendall Risk Mgmt.,* 246 F.R.D. 557, 566 (N.D. Ill. 2007) ("As a representative of the attorney, the attorney-client privilege extends to a paralegal acting as a subordinate to the attorney."); *Owens v. First Family Fin. Servs.,* 379 F. Supp. 2d 840, 848 (D. Miss. 2005) ("When a paralegal works on behalf of a lawyer who is representing a client, 'the attorney-client privilege applies with equal force to paralegals.'").

The interception by our government of Mr. Jumaev's phone call with his immigration attorney is not unique. In the prosecution of Reaz Qadir Khan, who is charged in the District of Oregon with conspiracy to provide material support, discovery provided to defendant Khan included a recorded call between Khan and his immigration attorney.[17] Furthermore, the government in Khan ultimately provided a number of recordings of Khan being interviewed as a witness by

[17] *See Memorandum in Support of Motion for Disclosure of Monitoring of Privileged Communications, Minimization Orocedures & Filter Team Protocol United States v. Kahn*, Case No. 3:12-cr-659-MO, (D. Or. April 28, 2014) (Doc. 190).

attorneys and investigators from the federal Public Defenders Office ("FPD") in connection with their defense of a client in a separate proceeding. The recordings disclosed information about the FPD's investigation and theories. The recordings were provided to the same prosecutor who prosecuted Khan and the FPD client. Since the conversations were not between an indicted individual and his counsel, the government felt free to listen to them. Still, the conversations did reveal the work product of the FPD and would normally be considered privileged, as addressed more fully below.

In addition to intercepting work product, the government has intercepted attorney-client communications occurring prior to indictment in other reported cases. For example, Robert Gottlieb was legal counsel for Adis Medunjanin, who was indicted in New York with terrorism-related charges involving an alleged attempt to bomb a New York City subway. Just before trial, Mr. Gottlieb was provided with a CD containing forty-two phone calls between him and Mr. Medunjanin. The calls all occurred before Mr. Medunjanin was formally charged. Mr. Gottlieb was never told why he was given access to the recordings, and he was unable to ascertain under what authority the government intercepted the calls.[18] Similarly, attorney Ron Kuby defended Ahmad Wais Afzali, who was also charged along with Mr. Medunjanin in the New York subway case. Calls between Mr. Kuby and Mr. Afzali were also intercepted.

In February 2014, new documents revealed that the communications of U.S.-based law firm Mayer Brown with its client, the government of Indonesia,

[18] *See* Nicolas Niarchos, *Has the NSA Wiretapping Violated Attorney-Client Privilege?*, The Nation, February 4, 2014, *available at* http://www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege.

came under surveillance by an Australian intelligence agency, which in turn provided the resulting intelligence to the United States. *See With Liberty to Monitor All, supra* at 56.

V. DEFENSE TEAM MEMBERS WILL NOT BE ADVISED BY THE GOVERNMENT THAT IT HAS INTERCEPTED THEIR COMMUNICATIONS AND METADATA WITHOUT AN ORDER FROM THIS COURT REQUIRING SUCH NOTICE.

A. Section 215

The statutory language of Section 215 only provides for notice to the recipient of the disclosure order. *See* 50 U.S.C. § 1861(d)(1)(A). Consequently, in the telephone metadata scenario, notice is only provided to the communications company. The statute only affords the communications company a mechanism to challenge the metadata collection. Furthermore, the communications company, as the recipient of the disclosure order, is prohibited from notifying its customers of the disclosure order. *See* 50 U.S.C. § 1861(d)(2).

B. Executive Order 12333

The Defense has not uncovered any information that the government has ever publicly disclosed its position as to whether there are any notice requirements with respect to interceptions obtained pursuant to EO 12333, and if so, what those requirements are. According to a New York Times article, the government's interpretation of its notice requirements would likely result in no notice being given to a criminal defendant, let alone his counsel.[19]

[19] *See* Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, New York Times, August 13, 2014 (stating that the government generally does not use evidence obtained through EO 12333 directly in criminal

The government's restrictive view of what notice is required by EO 12333, as well as its oft-articulated declination to provide Mr. Jumaev with FAA notice as detailed in the next section C, gives us no confidence that the government would advise us defense counsel if members of the Defense have been intercepted under the auspices of EO 12333.[20]

C. FISA and the FAA

50 U.S.C. § 1801(k) defines an "aggrieved person as follows: "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." The government has taken the position in this case that, with respect to Mr. Jumaev, disclosure will not be provided as to FAA material because Mr. Jumaev does not meet all of the criteria set forth in 50 U.S.C. § 1806 (f). This issue has been fully briefed in a number of previously filed pleadings.[21] In short, as to surveillance of the defense team, since the government has not indicted any member of the defense team, no notice of their having been intercepted under FISA will be provided to the Defense. Further,

---

proceedings specifically to avoid any requirement to disclose, and that "officials contend that defendants have no right to know if 12333 intercepts provided a tip from which investigators derived other evidence."), *available at* http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html.

[20] *See, e.g.,* Doc. 470 wherein the government relies on its interpretation of the FISA notice provisions to decline to affirmatively state whether information pertaining to Mr. Jumaev was obtained or derived from FAA related surveillance.

[21] *See* Docs. 458, 470, 499, and 525. To avoid repetition, Mr. Jumaev incorporates the relevant factual assertions and legal arguments set forth in those pleadings, namely, Doc. 458 at ,11-21, Doc. 470, at 2-6, Doc. 499 at 21-23, and Doc. 525 at 2-4.

because the government has argued that the notice requirement is identical under FISA and the FAA, no notice of FAA intercepts would likewise be provided to the Defense.

The government's unwillingness to comply with the notice requirements under the FAA has been well documented in this case. Mr. Muhtorov did not receive the notice to which he was clearly entitled until more than 20 months after his arrest. Mr. Muhtorov was the first criminal defendant to receive notice that FAA-derived evidence would be used against him. His notice was not provided until after the Solicitor General learned that he had incorrectly advised the Supreme Court in oral arguments in *Clapper v. Amnesty Int'l*, that such notice was routinely being provided to criminal defendants. To justify the failure to provide notice, the government advised the court:

> Prior to recent months, however, the Department had not considered the particular question of whether and under what circumstances information obtained through electronic surveillance under Title I or physical search under Title III could also be considered to be derived from prior collection under Title VII. After conducting a review of the issue, the Department determined that information obtained or derived from Title I or Title III FISA collection may, in particular cases, also be derived from prior Title VII collection, such that notice concerning both Title III and Title VII collections should be given in appropriate cases with respect to the same information.

(Doc. 559, at 9 n. 2).

The government's "explanation" has been repeated in other cases in which the required notice was not timely provided.[22] The government's excuse is

[22] Other cases in which notice was not provided include *United States v. Mohamud*, No. 3:10-cr-000474 (D. Or.) and *United States v. Qazi*, No. 12-60298 (S.D. Fla.) and *United States v. Hasbajrami,* No. 11-cr-623 (E.D.N.Y.); and *United States v. Mihalik*, No. 11-cr-00833 (C.D. Cal.).

inaccurate and unpersuasive. The ACLU has filed a civil suit pursuant to FOIA seeking the government's practices or policies for providing notice of FAA surveillance. That litigation has revealed that the government's claim that it had not "considered" the FAA notice issue until 2013 is demonstrably false. *See* Plaintiff's Memorandum of Law in Support of Their Cross-Motion for Summary Judgment and in Opposition to Defendant's Partial Motion for Summary Judgment, *American Civil Liberties Union v. United States Department of Justice*, at 1 (Doc. 24), No. 13 Civ. 7347 (GHW) (S.D.N.Y) (Aug. 22, 2014) ("ACLU Brief"). The issue was brought to DOJ's attention at least as early as 2011, when a defendant in another case filed a motion devoted to this precise question. *See* Motion to Clarify the Legal Authority Relied Upon by the Government to Conduct Electronic Surveillance, *United States v. Khan*, No. 11-cr-20331 (S.D. Fla. Dec. 14. 2011). Attorneys from the National Security Division of the Department of Justice participated in that case, as DOJ's filings in that case show. The issue was raised again in 2012, this time in the Supreme Court by the plaintiffs in *Clapper v. Amnesty Int'l*. Moreover, multiple 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.[23] Just because the Attorney General or Deputy Attorney General had not personally "considered" the issue until 2013—if that is really what DOJ means—

[23] *See* Savage, *supra* (explaining that NSD had "long used a narrow understanding of what 'derived from' means" to avoid providing notice").

is no basis for hiding what was, in reality, the controlling view within NSD for years.

To date, the government has not turned over any documents describing its notice policy, reiterating the ACLU's assertion that the government's "contention appears to be that the government did not have a notice policy before 2013 and that it does not have one now." *See* ACLU Brief, at 1.

In every case where the issue has been raised, the government has gone to great lengths to avoid its responsibility to provide notice. There is no reason to believe that notice will be provided to defense counsel unless this Court explicitly requires the government to provide the information requested herein.

VI. NOTICE IS NECESSARY TO ENSURE THAT MR. JUMAEV IS AFFORDED HIS SIXTH AMENDMENT RIGHTS AND TO ENSURE THAT THE FOURTH AMENDMENT RIGHTS OF MEMBERS OF THE DEFENSE TEAM ARE PROTECTED

This motion seeks to confirm that surveillance of the Defense members has occurred and continues to occur. Once the nature and scope of the surveillance is determined, Mr. Jumaev intends to file further pleadings challenging the legality of the specific types of surveillance that have been occurring. To that end, Mr. Jumaev will set forth here in general terms the legal framework describing the illegality of the government's interception of communications of the Defense. A more complete, detailed argument will be filed in a subsequent pleading once the exact nature of the surveillance has been disclosed.

A. Sixth Amendment Concerns

The attorney-client privilege is "one of the oldest recognized privileges for confidential communications." *Swindler & Berlin v. United States*, 524 U.S. 399, 403 (1998) (*citing Upjohn*, 449 U.S. at 389; (1981); *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888)).

The test to determine whether the attorney-client privilege exists has been stated thusly:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) unless the protection be waived.

United States v. Ruehle, 583 F.3d 600, 607 (9th Cir. 2009); *see also Steele v. First Nat'l Bank*, No. 90-1592-B, 1992 U.S. Dist. LEXIS 8501, at *4 (D. Kan. May 26, 1992) (applying test identical to that in *Ruehle*); *Alliance Constr. Solutions, Inc. v. Dep't of Corr.*,54 P.3d 861, 868 (Colo. 2002) ("the attorney-client privilege protects communications if: (1) the communication was made for the purpose of securing legal advice; (2) the person making the communication did so at the direction of his superior; (3) the superior requested that the communication be made so that the client could secure legal advice; (4) the subject matter of the communication was within the scope of the representative's duties; and (5) the communication was not disseminated beyond those persons, who because of the structure of the client's operations, needed to know its contents.").

As discussed above, the government has produced a phone call between Mr. Jumaev and his immigration lawyer's paralegal. This communication is clearly

privileged and the recording of the call is a blatant violation of Mr. Jumaev's attorney-client relationship with his immigration counsel.

The government's spying that allows it to discover the identity of persons whom Defense team members contacted, or did not contact, without the government's listening to the contents of such calls, violates the attorney work-product privilege. The government's accessing information of this nature is similar to determining the content of defense counsel's application for CJA services. For example, in *United States v. Gonzales*, No. CR 95-538-MV, 1997 WL 155403, 1997 U.S. Dist. LEXIS 4099 (D.C. N.M.) *modified on other grounds, United States v. Gonzales*, 150 F.3d 1246 (10th Cir. 1998), the court denied public access to CJA vouchers, stating that:

> The information on CJA cover forms, including the names and types of experts who have been consulted, persons who have been interviewed, subjects of research, and hours expended by counsel and experts on various issues, reveals basic information about the nature of defendant's trial strategy. Documentation submitted in support of claims attached to the cover forms is even more explicit in disclosing trial strategy. Even the absence of information may also reveal trial strategy: For instance, the failure of a defendant to hire a ballistics expert might mean that defendant will not dispute that a bullet found in a murder victim came from the defendant's gun."

U.S. Dist. LEXIS 4099, at *21-22.

The government violates the work-product doctrine[24] if it intercepts or inspects any defense team conversations regarding a case, including any

[24] The work product doctrine protects from adverse parties a civil or criminal defense attorney's strategy and thoughts about litigation. *United States v. Nobles*, 422 U.S. 225, 238-39 (1975). The work-product doctrine "is intended to preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategy 'with an eye towards litigation,' free from unnecessary intrusion by his adversaries." *United States v. Adlman*, 134 F.3d 1194, 1196 (2d Cir. 1998); *Genentech, Inc. v. United States Int'l Trade*

conversations with witnesses or prospective witnesses. *Gonzalez* clearly demonstrates how the government's acquisition of defense team telephone metadata obtained under Section 215, or any other program, reveals defense strategy, provides access to attorney work product, and violates Mr. Jumaev's Sixth Amendment rights.

Even if the data is not actually searched, knowing it is being collected has a chilling effect on the activities of the defense team as it tries to meet its constitutional and ethical obligations to effectively represent Mr. Jumaev. In addition to creating angst and concern among members of the Defense about communicating amongst themselves electronically, knowledge of the scope of government spying adversely affects the Defense's unfettered freedom to contact and interview potential witnesses, experts, and consultants. From defense counsels' point of view, the government's spying and surveillance pose the risk of disclosing defense strategy to the government. Also, ethical rules of professional conduct include the obligation to maintain confidentiality of certain information related to the representation of their clients. Attorneys should not have to risk being in violation of such rules simply because their client is charged with a specific type of offense.

Comm'n, 122 F.3d 1409, 1415 (Fed. Cir. 1997) (*"*"The work product privilege protects the attorney's thought processes and legal recommendations.'" (quoting *Zenith Radio Corp. v. United States*, 764 F.2d 1577, 1580 (Fed. Cir. 1985)). Protected work product includes "interviews, statements, memoranda, correspondence, briefs, mental impressions, personal beliefs, and countless other tangible and intangible" material. *Hickman v. Taylor*, 329 U.S. 495, 511 (1947). The work product privilege applies to all members of the defense team, not just the attorneys themselves. *Nobles*, 422 U.S. at 238-239 (holding doctrine protects material prepared by agents for the attorney as well as those prepared by the attorney himself). And, as discussed above, Rule16(b)(2)(a) expressly prohibits discovery of from discovery defense team's work product.

From the point of view of potential witnesses, many of whom already feel threatened given their religious beliefs, cultural background, and immigration status, meeting and communicating with counsel for an alleged terrorist, the documented scope and breadth of government surveillance greatly increases their reluctance to meet with counsel and openly share information. *See With Liberty to Monitor All*, *supra* at 59-61 (description by highly respected defense attorneys regarding the problems associated with dealing with both clients and witnesses in terrorism cases).

The government's collection of defense team metadata, and its ability of the government to perform sophisticated searches of the metadata, violates Mr. Jumaev's Sixth amendment rights. Even if searches of defense team metadata are not actually performed, defense team members' ability to conduct their communications in an effective manner is chilled by the knowledge that a search of their metadata is, as the *President's Review* stated is but a flick of the switch away.

B. Fourth Amendment Concerns

1. Section 215

Section 215 has been successfully challenged on constitutional grounds. In *Klayman v. Obama*, Judge Leon concluded that Klayman, a Verizon customer, had standing to challenge the constitutionality of Section 215. The court granted, but stayed, Klayman's request for injunctive relief, concluding there was a significant likelihood that Klayman would succeed in demonstrating that searches conducted pursuant to Section 215 were unreasonable for Fourth Amendment

purposes. The government has appealed. *See Klayman v. Holder,* No. 14-5208 (D.C.Cir.).

The *Klayman* court took the view that the metadata information was significantly greater than the information obtained by use of a pen register, which. is limited to the phone number dialed. "[T]he almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979." *Klayman v. Obama*, 957 F. Supp.2d at 33. In concluding that Klayman and the rest of us have a reasonable expectation of privacy in the metadata collected, Judge Leon relied heavily on the Supreme Court's ruling in *United States v. Jones*:

> This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring), that could not have been gleaned from a data collection in 1979.

Klayman, at 36. Finally, Judge Leon explicitly rejected the applicability of the "special needs doctrine" citing, among other things, the lack of documented success of the metadata program in stopping imminent attacks. *Id*. at 40-41.

Cases from other jurisdictions have not reached the same conclusion as the *Klayman* court. *See ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y.2013); *see also Smith v. Obama*, No. 2:13-CV-257-BLW, 2014 WL 2506421, 2014 U.S. Dist. LEXIS 76344 (D. Idaho June 3, 2014); *United States v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518, 2013 U.S. Dist. LEXIS 164038 (S.D.Cal. Nov. 18, 2013). The primary basis of the distinction between the holding of the

Klayman court and the other decisions is the question of an individual's reasonable expectation of privacy in the metadata. In *ACLU v Clapper, Moalin,* and *Smith* each court felt bound by the holding in *Smith v. Maryland*, 442 U.S. 735 (1979), in which the Supreme Court concluded that the defendant did not have a privacy interest in the numbers dialed from his phone which were obtained by law enforcement through a pen register. However, in *Smith v. Obama* the district court agreed that telephone metadata provided more information than the pen register at issue in *Smith v. Maryland*. The court felt constrained by the holding in *Smith v. Maryland* but stated that, "Judge Leon's decision [in Klayman] should serve as a template for a Supreme Court opinion. And it might yet." 2014 U.S. Dist. LEXIS 76344, at *11.

The court's analysis in *Moalin* did not delve as deeply into the issue as the court in *ACLU v. Clapper*. The *Moalin* court based its opinion on the holding in *Smith v. Maryland* that the metadata information was voluntarily provided by the caller to the phone company so there was no expectation of privacy. The court seemed to misconceive the type of information contained in metadata particularly when the data is analyzed using sophisticated computer programs. The court compared the metadata obtained under Section 215 with the pre-digital world going back to Samuel Morse and found no meaningful distinction. The court's analysis is not sustainable and is irreconcilable with all descriptions, even the government's, of the amount of information available through analysis of telephone metadata.

2. Executive Order 12333

Surveillance programs operated under EO12333 have never been reviewed by any court. Moreover, the programs are not governed by any statute. EO12333 was originally intended to apply to communications conducted outside the United States, i.e, communications that are not entitled to the same constitutional protections afforded U.S. persons communicating within the Untied States. Technological changes have changed the way communications are sent and stored. As a result, EO 12333 has a much greater likelihood of leading to the interception of communications and data of Americans. The *President's Review*, in discussing EO 12333, stated:

> Today, and unbeknownst to US users, websites and cloud servers may be located outside the United States. Even for a person in the US who never knowingly sends communications abroad, there may be collection by US intelligence agencies outside of the US.

President's Review, at 183. [25]

The warrantless interception of American citizens' communications implicates the Fourth amendment. The warrantless collection of metadata raises the same constitutional questions discussed with respect to Section 215 above. Notice of the nature of the information and/or data being collected is necessary to raise a properly focused challenge to these interceptions.

[25] The *President's Review* cited See Jonathan Mayer, "The Web is Flat" Oct. 30, 2013 (study showing "pervasive" flow of web browsing data outside of the US for US individuals using US-based websites), *available at* http://webpolicy.org/2013/10/30/the-web-is-flat/.

3. FISA and FAA

Constitutional challenges with respect to interceptions of Mr. Jumaev and Mr. Muhtorov made pursuant to FISA and the FAA have been addressed and briefed in several motions previously presented to this court.[26] The factual assertions and legal arguments set forth in the listed pleadings are applicable to communications of the Defense. Mr. Jumaev therefore incorporates the assertions and arguments set forth in the identified pleadings for purposes of this motion.

VII. CONCLUSION

In George Orwell's *1984, the* ubiquitous telescreens, dominating the city of Airstrip One, contained hidden microphones and cameras that allowed the Thought Police to spy upon everyone and thus identify anyone who might endanger the Party's regime. To many, the omnipresent government surveillance described in Orwell's 1949 fictional masterpiece is a part of the reality of our daily lives in this country. That doesn't make it right. And, it particularly doesn't make it right when it interferes with the constitutional protections afforded a criminally accused. In such an event, the only relief the accused can obtain from "Big Brother" is from the court

As a result and for the reasons set forth above, Mr. Jumaev first requests this Court issue an order requiring the government to provide notice whether communications of members of the Defense have been intercepted and whether metadata from communications by Defense members has been collected and/or

[26] *See supra* at n.12.

queried. Second, to make such notice sufficiently detailed to allow the Defense to make focused challenges of any interceptions and collection of data, the Defense moves the court to require the government to: describe what communications, metadata and other information have been collected, intercepted or surveilled and the period of time during which such collection, interception, or surveillance occurred. Third, to ensure that the government attorney tasked with providing such notice is not left in the awkward position in which the Solicitor General found himself after addressing the Supreme court in *Amnesty International v. Clapper*, the Defense moves the court to require the government to set forth with specificity the procedures employed by the government in determining whether counsel or other members of the defense team have been surveilled and whether their actual communications and/or metadata have been collected. Finally, the Defense moves the court to order the government to set forth minimization procedures used with respect to any communications or data collected, and the existence of a filter team and all filter team protocols, that have been used or are currently being utilized by the government in this case, and for such further relief as the Court may deem proper.

Dated, this 20th day of October 2014.

Respectfully submitted,

s/David B. Savitz
David B. Savitz
1512 Larimer Street, #600
Denver, CO 80202
303-825-3109
303-830-0804 (fax)
SavMaster@aol.com

s/Mitchell Baker
Mitchell Baker
1543 Champa Street, Suite 400
Denver, CO 80202
(303) 592-7353
mitchbaker@estreet.com

(*Attorneys for Defendant Bakhtiyor Jumaev*)

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 20th day of October, 2014 I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to counsel of record:

Gregory A. Holloway
Email: Gregory.Holloway@usdoj.gov

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

Warren Richard Williamson
Office of the Federal Public Defender
Counsel for Jamshid Muhtorov
Email: Rick_Williamson@fd.org

Brian Rowland Leedy
Office of the Federal Public Defender
Counsel for Jamshid Muhtorov
Email: Brian_Leedy@fd.org

Kathryn J. Stimson
Counsel for Jamshid Muhtorov
Email: kathryn@stimsondefense.com

Patrick Toomey
American Civil Liberties Union
Counsel for Jamshid Muhtorov
Email: ptoomey@aclu.org

s/Pat Austin
Pat Austin, Paralegal to David B. Savitz