HOLLY A. SULLIVAN
California State Bar No.216376
110 West C Street, Suite 1903
San Diego, California 92101
Telephone: (619) 269-8054
Fax: (619) 794-2263
Email: hollyasullivan@yahoo.com

Attorneys for Basaaly Moalin

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

(HONORABLE JEFFREY T. MILLER)

UNITED STATES OF AMERICA Plaintiff, v. BASAALY MOALIN, Defendant.	Case No. 10-CR-4246 (JM) Date: September 30, 2013 Time: 9:00 a.m. STATEMENT OF FACTS AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF JOINT MOTION PURSUANT TO RULE 33, FED. R.CRIM. P., FOR A NEW TRIAL

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

Introduction

This Memorandum of Law is submitted on behalf of defendants Basaaly Moalin, Mohamed Mohamed Mohamud, Issa Doreh, and Ahmed Nasir Taalil Mohamed in support of their motion, pursuant to Rule 33, Fed.R.Crim.P., for a new trial in the above-captioned case, in which they were convicted after a jury trial February 22, 2013.

The motion is based upon disclosures made recently – since the June 2013 commencement of reporting on material provided by Edward Snowden regarding surveillance programs operated by the U.S. government through the National Security Agency ("NSA") – by U.S. officials from the Federal Bureau of Investigation ("FBI") and NSA in Congressional testimony and other forums.

As discussed below, among the disclosures by those government officials was that such NSA collection, storage, and surveillance were instrumental in the investigation in this case. Indeed, ultimately, U.S. government officials have cited this case as the only U.S. criminal case in which a particular NSA program produced information vital to the prosecution.

The collection/storage/interception cited by the government officials relates to Mr. Moalin's telephone contacts in 2007, after a prior investigation of him years earlier had been closed due to lack of sufficient evidence to institute any charges. At issue in this motion is the legality of that collection/storage/interception, and its impact on this case, including not only the manner in which evidence was obtained and used by the government, and whether other evidence constitutes the "fruit of the poisonous tree," but also the viability of the government's only theory at trial. Further at issue is whether NSA, or other U.S. government agencies, are in possession of exculpatory or discoverable material to which defendants were entitled in advance of trial.

In addition, certain 3500 material alluded to *other*, subsequent electronic surveillance of Mr. Moalin's communications while the FISA wiretap on his phone was in progress – surveillance which, due to its real-time monitoring, indicates it was not pursuant to the same NSA program that collected the other information related to Mr.

Moalin (and the subject of the recent official statements), but instead was conducted under the auspices of another statutorily and constitutionally invalid NSA program.

This Rule 33 motion also seeks discovery of the data and information collected/stored/intercepted by NSA, and to which the U.S. government officials have referred in their public statements, and/or which appears in 3500 material. If that information is classified, it is submitted that it should be produced to cleared counsel (as each defendant in this case is represented by at least one cleared counsel).

Thus, this Rule 33 motion raises the following specific issues, the favorable resolution of which would be sufficient to grant a new trial:

(1) whether the NSA interception and/or collection of Mr. Moalin's communications violated his Fourth and First Amendment rights, and/or violated the Foreign Intelligence Surveillance Act ("FISA"), or any other statutory authority upon which such interception/collection was purportedly based;

(2) whether the government's response to Mr. Moalin's motion challenging the electronic surveillance and physical searches conducted pursuant to FISA – which response was filed *ex parte* – was complete and accurate with respect to the scope of electronic surveillance and collection to which Mr. Moalin was subjected;

(3) whether that government response (and any other related government submissions), as well as the underlying FISA applications and submissions in support thereof, should be provided to cleared defense counsel pursuant to either 50 U.S.C. §§1806(f) & (g), and/or the Fifth Amendment's Due Process clause; and whether the government's submissions pursuant to §4 of the Classified Information Procedures Act ("CIPA"), and the underlying materials, should be disclosed to cleared defense counsel; and whether the Court should revisit its review and decisions with respect to any of the government's applications made

pursuant to CIPA §4, and provide the government's CIPA §4 submissions to cleared defense counsel;

(4) whether the government failed to provide Rule 16 discovery – the evidence of Moalin's communications as evidenced by the NSA interceptions and collection of metadata – it was obligated to produce to Mr. Moalin;

(5) whether the public statements, including Congressional testimony of certain FBI and NSA officials, materially undermines the government's central and indispensable premise at trial: that the intercepted conversations were between Moalin and Aden Hashi Ayrow *directly*, and *not in*directly; and

(6) whether the government failed to provide *Brady* material in the form of:

(a) the reasons underlying the conclusion, at the end of the initial 2003 investigation of Mr. Moalin, that he was not engaged in illegal conduct or linked to terrorism. Also, that earlier investigation likely yielded abundant, if not conclusive, evidence that Mr. Moalin was sending money to Somalia for humanitarian and other (family) purposes even before *al Shabaab* existed, and that he did not harbor anti-U.S. or pro-terrorist sympathies;

(b) evidence that Mr. Moalin's contacts with *al Shabaab* that precipitated the current investigation were *in*direct, and not directly with Mr. Ayrow;

(c) exculpatory information and material related to the FBI's April 2009 Field Intelligence Group Assessment of Mr. Moalin, which Mr. Moalin requested in his pretrial motions; and,

(d) anything exculpatory generated by and during the earlier Anaheim investigation referred to in Ahmed Nasir's Pre-Sentence Report ("PSR") – which also apparently resulted in a declination of

charges.

Accordingly, it is respectfully submitted that the Court should grant defendants' Rule 33 motion, and order a new trial, and/or compel the discovery demanded in this motion, and/or conduct the evidentiary hearings requested herein.

Statement of the Facts

A. *The Charges, Trial, and Verdict*

The Superseding Indictment, S2 10 Cr. 4246 (JM) contained five counts, alleging a Conspiracy to Provide Material Support for Terrorism, in violation of 18 U.S.C. §2339A(a) (Count One); Conspiracy to Provide Material Support to a Foreign Terrorist Organization ("FTO"), in violation of 18 U.S.C. §2339B(a)(1) (Count Two); Conspiracy to Kill in a Foreign Country, in violation of 18 U.S.C. §956 (Count Three); Conspiracy to Launder Monetary Instruments, in violation of 18 U.S.C. § 1956(a)(2)(A) and (h) (Count Four); and Providing Material Support for Terrorism, in violation of 18 U.S.C. § 2339A(a) Count Five).

All four defendants were charged in Counts One, Two, and Three. Count Four charged Mr. Moalin alone, and Count Five charged all defendants *except* Mr. Ahmed Nasir.

Trial commenced January 28, 2013. In its opening statement, the government argued that "[y]ou'll learn in this case that he was the direct connection to Aden Ayrow, the *al-Shabaab* leader who told him it was time to finance the jihad." Trial Transcript, January 30, 2013, at 5. *See also id*., at 7 ("[a]nd this is how it would work. Aden Ayrow, *al-Shabaab* leader, rock star in *al-Shabaab* and in Somalia, both inside and outside of Somalia, would talk to Basaaly – again, the main connection to Aden Ayrow . . ."); at 10 ("[i]n January of 2008 Aden Ayrow is talking to Basaaly").

Throughout the trial, the government's theory remained consistent with that declaration: that the person named "Sheikalow" in the recorded telephone conversations was, in fact, Mr. Ayrow, and that Mr. Moalin communicated directly with Mr. Ayrow for the purpose of providing material support, in the form of financial assistance, to *al*

Shabaab, a designated Foreign Terrorist Organization ("FTO").

Thus, in summation the government contended that "Basaaly Moalin was on the phone with Aden Ayrow, personally on the phone with this internationally infamous terrorist leader." Trial Transcript, February 19, 2013, at 4. *See also id*., at 5 ("[n]ow, I am going to review with you all the bread crumbs – really not bread crumbs – all the neon lights that point to the inescapable conclusion that this Sheikalow, the Majadhub, on the phone with Basaaly Moalin, that was Aden Ayrow").

The jury returned a verdict of guilty on all counts against all defendants February 22, 2013. All four defendants, who were remanded pending trial, remain in custody.

B. ***Mr. Moalin's Pretrial Motion to Suppress Electronic Surveillance Conducted Pursuant to FISA and the FISA Amendments Act***

Mr. Moalin moved pretrial to suppress the fruits of the FISA electronic surveillance and search(es). *See* Docket #92 (December 9, 2011), at 6-28.[1] As part of that motion, Mr. Moalin moved to preclude any interceptions conducted pursuant to FISA generally, as well as to any such surveillance requested and conducted pursuant to the authority provided in 50 U.S.C. §1881a, enacted in 2008 as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008) (hereinafter "FAA"), or to discover whether any information in the FISA applications was the product of surveillance authorized under the FAA. *See* Docket # 92, at 17-18.

Since the FISA surveillance of Mr. Moalin's telephone straddled the date of §1881a's enactment, with some occurring in late 2007, and the remainder until December 2008, it was unknown to Mr. Moalin (and remains unknown) whether any of the FISA electronic surveillance was conducted pursuant to the FAA. *Id*., at 17. Mr. Moalin also sought, via 50 U.S.C. §§1806(f) & (g) disclosure of the underlying FISA applications and supporting materials.

The factual portion of the government response to Mr. Moalin's motion was

[1] The government had previously filed a Notice of Intent to Use FISA Information. *See* Docket #s 12 & 44.

submitted *ex parte* February 23, 2012, and remains so. *See* Docket #128. Mr. Moalin filed a Reply March 9, 2012, related to the legal argument advanced by the government in its publicly filed opposition to the motion. *See* Docket #131.

In adjudicating the motion, the Court first issued an *ex parte* Order June 4, 2012, Docket #146, that has never been provided to the defense (either cleared counsel or the defendants). Apparently the Court's Order required some action or response by the government, which moved initially for an extension of time to comply with the Court's June 4, 2013, Order. *See* Docket #148 (June 15, 2012). The Court granted that application (*see* Docket #149), and June 27, 2012, the government filed an *ex parte* Statement In Compliance with the Court's June 4, 2012, Order. *See* Docket #151. Again, neither defendants nor their counsel have been afforded access to that Statement, or the Order to which it related.

C. ***Mr. Moalin's Pretrial Motion for Production of Exculpatory Material and Information***

In his pretrial motions, Mr. Moalin moved for production of exculpatory material the government was obligated to provide under *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny. *See* Docket #92, at 34-36. In large part, the specifics of the motion were based on an FBI San Diego Field Intelligence Group Assessment, dated June 15, 2011 (hereinafter "FIG Assessment").

That FIG Assessment was summarized in a two-page partially redacted FBI Report dated June 15, 2011, created by the San Diego office (denominated in discovery as GA-DOCS-000051-52, and attached hereto as Exhibit 1). *Id.*

According to the FIG Assessment:

> [t]he San Diego FIG assesses that Moalin, who belongs to the Hawiye tribe/Habr Gedir clan/Ayr subclan, is the most significant al-Shabaab fundraiser in the San Diego Area of Operations (AOR). Although Moalin has previously expressed support for al-Shabaab, he is likely more attentive to Ayr subclan issues and is not ideologically driven to support al-Shabaab. The San Deigo FIG assesses that Moalin likely supported now deceased senior al-Shabaab leader Aden Hashi Ayrow due to Ayrow's tribal affiliation with the Hawiye tribe/Habr Gedir clan/Ayr subclan rather than his position in al-Shabaab. Moalin has also worked diligently to support Ayr

> issues to promote his own status with Habr Gedir elders. The San Diego FIG assesses, based on reporting that Moalin has provided direction regarding financial accounts to be used when transferring funds overseas that he also serves as a controller for the US-based al-Shabaab fundraising network.

Id. (Exhibit 1).

Mr. Moalin's motion for *Brady* material also referenced prior investigations of Mr. Moalin, and sought exculpatory information and material regarding them as well. *See* Docket #92, at 34-36.

D. ***Recent Disclosures By U.S. Government Officials Regarding NSA Interception/Collection of Mr. Moalin's Electronic Communications***

In its June 8, 2013, edition, *The Washington Post* published the first in a continuing and ongoing series of articles by a variety of news organs, including *The Guardian* and *The New York Times*, detailing disclosures by Edward Snowden, a former NSA contract employee. The documents Mr. Snowden provided revealed the existence of the scope of NSA's electronic surveillance, interception, and collection, including communications data relevant to U.S. persons.[2]

Two aspects of those revelations would seem to be particularly relevant here: (1) the collection, storage, and subsequent retrospective use of metadata gleaned from electronic communications by U.S. persons in the U.S., pursuant to Section 215 (50 U.S.C. §1861); and (2) the interception of electronic communications, particularly those with a domestic U.S. component (sending or receiving or, in some cases, entirely), pursuant to Section 702 (50 U.S.C. §1881a) of the FAA.[3]

In response to the Snowden/ *Washington Post* disclosures, Congressional

---

[2] Three days earlier, June 5, 2013, *The Guardian* published an article regarding a previously undisclosed order by the Foreign Intelligence Surveillance Court, but Mr. Snowden was not cited as the source (although apparently he provided that document as well). *See* Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013, available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order - article.

[3] Those two sections are discussed in more detail **post**, in POINT I.

hearings were convened on the subject within two weeks. During a June 18, 2013, appearance before the House Permanent Select Committee on Intelligence ("HPSCI"), Sean Joyce, Deputy Director, FBI, testified regarding criminal cases that had been initiated as a result of the NSA interception/collection programs.

Initially, in his prepared remarks, Deputy Director Joyce informed the panel about a particular case which he did not identify. He said of this case that

> the FBI had opened an investigation shortly after 9/11. We did not have enough information nor did we find links to terrorism, so we shortly thereafter closed the investigation. However, the NSA, using the business record FISA, tipped us off that this individual had indirect contacts with a known terrorist overseas. We were able to reopen this investigation, identify additional individuals through a legal process and were able to disrupt this terrorist activity.

Transcript, HPSCI Hearing, June 18, 2013, at 9-10. (A copy of the transcript of that hearing is attached hereto as Exhibit 2).

Later in that same session, during the question and answer period, Deputy Director Joyce confirmed that the case to which he had referred was *this* case: *United States v. Moalin*, and that the individual who was the subject of the initial (closed) investigation, and whose phone records had been the subject of Section 215 collection and storage, was Mr. Moalin. Asked by Rep. Mac Thornberry (R-Tex.) to describe the Moalin case further, Gen. Keith Alexander (USA), NSA's Director, deferred to Deputy Director Joyce, "because the actual guys who actually do all the work when we provide it is the FBI and get [the description] exactly right." *Id*., at 18 (Exhibit 2).

As a result, Deputy Director Joyce explained that

> It was a(n) investigation after 9/11 that the FBI conducted. We conducted that investigation and did not find any connection to terrorist activity. Several years later, under the 215 business record provision, the NSA provided us a telephone number only in San Diego that had indirect contact with an extremist outside the United States. We served legal process to identify who was the subscriber to this telephone number. We identified that individual. We were able to, under further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA Court, we were able to identify co-conspirators, and we were able to disrupt this terrorist activity.

Id., at 18-19 (Exhibit 2).[4]

Four weeks later, at a July 18, 2013, address at the Aspen Security Forum in Aspen, Colorado, Gen. Alexander repeated that same account of this case:

> . . . so from some information we got in Somalia, we saw some – we looked at a phone number, we said we know this is associated with *al Qaeda*, we looked at that phone number and we saw it touched a phone number in San Diego. And [Deputy Director] Joyce . . . was the one who said that was [Basaaly Moalin] case that they had started in 2003 but didn't have enough information to go up on. In 2007, we saw him talking to a facilitator in Somalia. We passed – all we have is the number. We don't know who it – a nine-digit number [or] ten-digit number. We pass that – I guess they're ten digits – we're going to be accurate – a 10-digit number to them. And they look at that and they go, ooh, this is [Basaaly Moalin]. They look up and said, four years ago we had a case. They reopened the case.

Transcript, July 18, 2013, Aspen Security Forum, Gen. Keith Alexander, at 5. (A copy of that transcript is attached hereto as Exhibit 3). *See also* Transcript, July 31, 2013, Black Hat USA 2013 Conference, Las Vegas, Nevada, Gen. Keith Alexander, at 3-4. (A copy of that transcript is attached hereto as Exhibit 4).[5]

---

[4] *See also* Marshall Curtis Erwin and Edward C. Liu, *NSA Surveillance Leaks: Background and Issues for Congress*, Congressional Research Service, July 2, 2013, R43134, at 11, available at http://www.fas.org/sgp/crs/intel/R43134.pdf ("**Basaaly Saeed Moalin**: NSA, using phone records pursuant to *215 authorities*, provided the FBI with a phone number for an individual in San Diego who had indirect contacts with extremists overseas. The FBI identified the individual as [Mr. Moalin] and determined that he was involved in financing extremist activity in Somalia") (emphasis in original) (footnotes omitted).

[5] At the Black Hat conference, Gen Alexander recounted that

> we gave [the FBI the California telephone number] in 2007. In 2004, they had ordered an investigation on that individual, but did not have enough information to open a full field investigation, so they closed that investigation down. In 2007, with the number we gave them, they had enough information. They take that number, and now their portion of this is they can take a national security (clip?), find out who that number belongs to, and they found out it was Basaaly Moalin. They can then, with

Deputy Director Joyce, appearing before the Senate Judiciary Committee July 31, 2013, reiterated during his testimony the genesis and chronology of the investigation in this case:

> another instance when we used the business record 215 program, as Chairman – Leahy mentioned, [Basaaly Moalin]. So, initially, the FBI opened a case in 2003 based on a tip. We investigated that tip. We found no nexus to terrorism and closed the case.
>
> In 2007, the NSA advised us, through the business record 215 program, that a number in San Diego was in contact with an Al-Shabaab in East Al Qaida – East – Al Qaida East Africa member in Somalia. We served legal process to identify that unidentified phone number. We identified [Mr. Moalin].

Transcript, July 31, 2013, Senate Judiciary Committee, Deputy Director Sean Joyce, at 14. A copy of the transcript is attached hereto as Exhibit 5.

In addition to the recent disclosures, the 3500 material for the government's linguist, Liban Abdirahman, at GA-ABDIRAHMAN-000006 (and attached as Exhibit 6 hereto), includes a January 24, 2008, e-mail from a redacted source (probably FBI Special Agent Michael C. Kaiser, the case agent) that states, "We just heard from another agency that Ayrow tried to call Basaaly today, but the call didn't go through." As noted **post**, that raises the additional question whether Mr. Moalin was subject to other means of interception, *i.e.*, Section 702 (FAA §1881a), conducted by NSA even while the FBI's FISA wiretap was underway.

> probable cause, get a [FISA] warrant. NSA only has the fact of a number. FBI could take that, see where it connects to, use a national security letter and the legal authorities given to them to take the next step.

Transcript, July 31, 2013, Black Hat USA 2013 Conference, Las Vegas, Nevada, Gen. Keith Alexander, at 3-4 (Exhibit 4).

ARGUMENT

I. *The NSA's Interception and/or Collection of Data Related to Mr. Moalin's Electronic Communications, or Any Aspect of the Communications Themselves, Violated the First and Fourth Amendments, FISA, or Other Claimed Statutory Authority*

Both Section 215 (50 U.S.C. §1861) and Section 702 (50 U.S.C. §1881a) – to the extent either or both were employed to conduct electronic surveillance on Mr. Moalin, and/or to collect and store or intercept his communications – are unconstitutional as applied to Mr. Moalin in this case.

The various means by which those provisions violate FISA itself, as well as the First and Fourth Amendments, is treated most comprehensively in papers filed by the American Civil Liberties Union in two separate lawsuits instituted with respect to those two sections. In *Amnesty International USA, et al. v. Clapper*, 08 Civ. 06259 (JGK) (S.D.N.Y.), the plaintiffs challenged Section 702 (50 U.S.C. §1881a) in a civil declaratory judgment action. Ultimately, the Supreme Court ordered dismissal of that action because plaintiffs therein lacked standing. *See Clapper v. Amnesty International USA*, ___ U.S. ___, 133 S. Ct. 1138 (2013).

In *American Civil Liberties Union, et al. v. Clapper*, 13 Civ. 03994 (WHP) (S.D.N.Y.), the plaintiffs have challenged the use of Section 215 (50 U.S.C. §1861) as described in the recent disclosures by Mr. Snowden and confirmed by government officials and documents. That action remains pending.

Rather than simply repeat the comprehensive and compelling statutory and constitutional analysis performed in ACLU's papers, defendants respectfully incorporate them by reference herein and adopt them from the following pleadings in those cases: (a) in *Amnesty International USA*, Docket #7, at 15-53 (attached hereto as Exhibit 7); and (b) in *ACLU*, Docket # 26, at 8-36 (attached hereto as Exhibit 8).

However, this motion will set forth some of the factual background with respect to each section to provide sufficient context, and will also discuss certain Fourth Amendment principles that are not addressed in the ACLU's briefs.

A. *Collection and Storage Via Section 215 of the USA PATRIOT Act (50 U.S.C. §1861)*

1. *The Origins and Evolution of Section 215 (50 U.S.C. §1861)*

In enacting FISA in 1978, Congress created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny government applications for surveillance orders in foreign-intelligence investigations. *See* 50 U.S.C. § 1803(a). The FISC meets in secret, generally hears argument only from the government, and rarely publishes its decisions. *See, e.g.*, FISC R. P. 17(b), 62. *See also* http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

Section 215 (18 U.S.C. §1861), was originally added to FISA in 1998. *See* 50 U.S.C. §§1861-1862 (2000 ed.). In its initial form, it permitted the government to compel the production of certain records in foreign-intelligence or international-terrorism investigations from common carriers, public-accommodation facilities, storage facilities, and vehicle rental facilities. *Id.* at §1862 (2000 ed.). The government was required to include in its application to the FISC "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power." *Id*.

The USA PATRIOT Act and several successor bills modified that provision in several respects.[6] In its current form, the statute – commonly referred to as Section 215 – allows the government to obtain an order requiring the production of "any tangible things" upon a "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Id.*

---

[6] The "PATRIOT Act" is the name customarily used to refer to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56. *See also* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. 107-108 (2001); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177 (2006).

§1861(b)(2)(A). The provision deems certain kinds of tangible things "presumptively relevant."[7]

While the amendments to this provision expanded the government's investigative power, that expansion was not without limits. Language added by the Patriot Act prohibits the government from using the provision to obtain tangible things that could not be obtained through analogous mechanisms. It states: "An order under this subsection . . . may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." *Id.*, §1861(c)(2)(D).

Until recently, the public knew little about the government's use of Section 215. In 2011, however, Senators Ron Wyden and Mark Udall, both of whom sit on the Senate Select Committee on Intelligence, stated publicly that the government had adopted a "secret interpretation" of Section 215, and predicted – quite correctly now in hindsight– that Americans would be "stunned," "angry," and "alarmed" when they learned of it.[8]

Their efforts to make more information available to the public, however, were largely unsuccessful, as were parallel efforts under the Freedom of Information Act. Ordinary citizens who wanted to understand the government's surveillance policies were entirely reliant on the government's own statements about them, and those statements were sometimes misleading or false. *See, e.g.*, Glen Kessler, "James Clapper's 'Least Untruthful' Statement to the Senate", *Wash. Post*, June 12, 2013, available at

---

[7] *See* 50 U.S.C. § 1861(b)(2)(A) (deeming tangible things "presumptively relevant to an authorized investigation" if they pertain to "a foreign power or an agent of a foreign power;" "the activities of a suspected agent of a foreign power who is the subject of such authorized investigation;" or "an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation").

[8] 157 Cong. Rec. S3386 (daily ed. May 26, 2011) (statement of Sen. Ron Wyden); 157 Cong. Rec. S3389 (daily ed. May 26, 2011) (statement of Sen. Mark Udall).

http://wapo.st/170VVSu (discussing statement by the Director of National Intelligence indicating, falsely, that government was not collecting information about millions of Americans).

2. *The NSA's Mass Call-Tracking Program*

In its June 5, 2013, edition, *The Guardian* disclosed a previously secret FISC order, labeled a "Secondary Order," directing Verizon Business Network Services ("Verizon") 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 its network between April 25, 2013 and July 19, 2013.[9] The Secondary Order specified that telephony metadata includes, for each phone call, the originating and terminating telephone number as well as the call's time and duration. Secondary Order at 2. On the day the Secondary Order expired, the Director of National Intelligence issued a statement indicating that the FISC had renewed it. Office of the Dir. of Nat'l Intelligence, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata* (July 19, 2013), http://1.usa.gov/12ThYlT.

The government has disclosed that the Secondary Order was issued as part of a broader program that has been in place for seven years that involves the collection of information about virtually every phone call, domestic and international, made or received in the United States. *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act*, (Aug. 9, 2013), http://bit.ly/15ebL9k ("White Paper"); Dep't of Justice, Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization (Feb. 2, 2011),

---

[9] Secondary Order at 2, *In re Application of the FBI for an Order Requiring the Production 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 (FISA Ct. Apr. 25, 2013)) ("Secondary Order"). Within the days after *The Guardian* disclosed the Secondary Order, DNI Director Clapper acknowledged its authenticity. *See* Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013), http://1.usa.gov/13jwuFc.

http://1.usa.gov/1cdFJ1G. The Secondary Order to Verizon was issued pursuant to a "Primary Order" that the government has now released and that sets out procedures the NSA must follow to "query" telephony metadata collected under the Secondary Order.[10]

The Primary Order and the administration's White Paper explain how the government analyzes and disseminates information housed in the massive database assembled by the call-tracking program. Specifically, the documents indicate that the NSA is permitted to query this database when a "designated approving official" at the NSA determines that "there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with" a "foreign terrorist organization." Primary Order at 7.[11] The NSA is permitted to review not just telephony metadata pertaining to the NSA's specific target, but also telephony metadata pertaining to individuals as many as three degrees removed from that target.

Under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as "hops"). The first "hop" refers to the set of numbers directly in contact with the initial or "seed" identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers. White Paper at 3–4.

Even assuming, conservatively, that each person communicates by telephone with forty different people, an analyst who accessed the records of everyone within three hops of an initial target would have accessed records concerning more than two million

---

[10] Primary Order at 3, 6–11, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-80 (FISA Ct. Apr. 25, 2013)) ("Primary Order").

[11] The government has acknowledged that the NSA has violated the Primary Order's restrictions on multiple occasions. White Paper at 5 ("[s]ince the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered as a result of DOJ and ODNI reviews and internal NSA oversight").

people. The government has disclosed that the NSA conducted queries on approximately 300 selectors in 2012 alone. White Paper at 4.

The NSA stores the information collected under the program for five years.[12] Its collection of telephony metadata continues "on an ongoing daily basis." Secondary Order at 2.

B. *The NSA's Interceptions Via Section 702 (50 U.S.C. §1881a)*

The historical background of Section 702 (50 U.S.C. §1881a) is set forth in detail in Exhibit 7, at 3-10, and is adopted and incorporated by reference herein. Before passage of the FAA, FISA generally foreclosed the government from engaging in "electronic surveillance" without first obtaining an individualized and particularized order from the FISC. The government was required to submit an application that identified or described the target of the surveillance; explained the government's basis for believing that "the target of the electronic surveillance [was] a foreign power or an agent of a foreign power;" explained the government's basis for believing that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power;" described the procedures the government would use to "minimiz[e]" the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons; described the nature of the foreign intelligence information sought and the type of communications that would be subject to surveillance; and certified that a "significant purpose" of the surveillance was to obtain "foreign intelligence information." *Id.* § 1804(a) (2006).

"Foreign intelligence information" was defined broadly (and is still defined broadly) to include, among other things, information concerning terrorism, national security, and foreign affairs, and the FISC could issue such an order only if it found, *inter*

---

[12] *See* Dep't of Justice, *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization* 4 (Feb. 2, 2011), http://1.usa.gov/1cdFJ1G; Siobhan Gorman & Julian E. Barnes, "Officials: NSA Doesn't Collect Cellphone-Location Records," *Wall St. J.*, June 16, 2013, available at http://on.wsj.com/13MnSsp.

alia, "probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power," *id*. § 1805(a)(2)(A); and that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power," *id*. § 1805(a)(2)(B).

In August 2007, Congress enacted the Protect America Act, Pub. L. No. 110-55 (2007). The Act expanded the executive's surveillance authority and provided legislative sanction for surveillance that the President had previously been conducting since 2001 under the warrantless Terrorist Surveillance Program ("TSP").

However, due to a "sunset" provision under which the amendments enacted within the Protect America Act ceased to have effect on February 17, 2008, Congress passed permanent revisions to FISA through the FAA, which President Bush signed into law July 10, 2008. While leaving FISA in place insofar as communications *known* to be purely domestic are concerned, the FAA revolutionized the FISA regime by allowing the mass acquisition of U.S. citizens' and residents' international telephone and e-mail communications.

Under section 702(a) (50 U.S.C. §1881a(a)), the Attorney General and DNI can "authorize jointly, for a period of up to one year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."

While the FAA prohibits the government from, *inter alia*, "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," *id*. § 702(b)(1), an acquisition authorized under section 702(a) (50 U.S.C. §1881a(a)) may encompass the international communications of U.S. citizens and residents. Indeed, the Attorney General and the DNI may authorize a mass acquisition under section 702(a) even if *all* communications to be acquired under the program originate or terminate inside the United States.

The FAA does not require the government to demonstrate to the FISC that its surveillance targets are foreign agents, engaged in criminal activity, or connected even

remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, e-mail addresses, places, premises, or property at which its surveillance will be directed. FAA §702(g)(4) (50 U.S.C. §1881a(g)(4)).

Thus, the government may obtain a mass acquisition order without identifying the people (or even the group of people) to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without specifying the particular communications to be collected; without obtaining individualized warrants based on criminal or foreign intelligence probable cause; and without making even a prior administrative determination that the acquisition relates to a particular foreign agent or foreign power.

A single mass acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents. Equally striking is the Act's failure to place meaningful limits on the government's retention, analysis, and dissemination of information that relates to U.S. citizens and residents. While the Act requires the government to adopt "minimization procedures" that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination of nonpublicly available information concerning unconsenting United States persons," the statute contemplates minimization procedures that are generic and programmatic, rather than tailored to the surveillance of individualized targets.

Moreover, the statute does not prescribe specific minimization procedures, does not give the FISA court any authority to oversee the implementation of the procedures, and specifically allows the government to retain and disseminate information – including information relating to U.S. citizens and residents – if the government concludes that it is "foreign intelligence information." FAA § 702(e) [referencing 50 U.S.C. §§1801(h)(1) & 1821(4)(A)]. Nothing in the Act forecloses the government from compiling databases of such "foreign intelligence information" and searching those databases for information about specific U.S. citizens and residents. Again, the statute

defines the phrase "foreign intelligence information" exceedingly broadly.

The role of the FISC in authorizing and supervising surveillance conducted under the FAA is "narrowly circumscribed." *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted). The FISC is required to issue a mass acquisition order if it finds that the government's certification "contains all the required elements" and that the "targeting and minimization procedures" are consistent with the requirements of the statute and the Fourth Amendment. FAA § 702(i)(3)(A) (50 U.S.C. §1881(i)(3)(A)).

The FISC does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not supervise the implementation of the government's targeting or minimization procedures. Moreover, even if the FISC rejects the government's certification or procedures, the government "may continue" its surveillance activities during the pendency of any appeal or further court proceedings. *Id*., §702(i)(4)(B) (50 U.S.C. §1881(i)(4)(B)). The FAA thereby permits the government to continue its surveillance activities even if the FISC has concluded that those activities are inconsistent with the statute or are unconstitutional.

C. *Applying the Statutory and Constitutional Analysis to Mr. Moalin and This Case*

1. *Mr. Moalin Was Subject to the Ultimate "Big Brother" Abuse of the NSA's Untrammeled License to Conduct Electronic Surveillance and Collection*

Here, the worst-fears nightmare electronic surveillance/metadata collection scenario has occurred: a U.S. citizen – Mr. Moalin – located *in the U.S.* was subject to an initial investigation that U.S. law enforcement and intelligence officials acknowledge did not yield evidence of "links to terrorism," yet information collected about his electronic communications, *i.e.*, his telephone number, was nevertheless stored in a massive database and provided by NSA to the FBI four years later for solely retrospective use. That use lead directly to targeted FISA electronic surveillance (which U.S. officials concede could not have been authorized without that stored information) and, ultimately, this indictment and conviction.

Thus, despite the conclusion that Mr. Moalin had not broken any laws, or had any "nexus" or "links to terrorism," or "connection to terrorist activity," his information, absent probable cause, remained "seized" by the government for unfettered use indefinitely. This scenario manifests precisely the most acute concerns articulated with respect to the scope and duration of NSA collection and interception: a perpetual database on persons cleared of wrongdoing, unhinged from any standard designed to hold intelligence-gathering accountable to the Fourth or First Amendments.

2. *The Section 215 Collection and Storage Lacked the Requisite "Particularity" and Constituted an Impermissible "General Warrant"*

In addition to the constitutional infirmities detailed in Exhibit 8, the lack of any specificity in the standards governing the collection and/or storage of information related to Mr. Moalin pursuant to Section 215 (50 U.S.C. §1861) renders it invalid as a "general warrant," and/or lacking in the necessary "particularity" the Fourth Amendment demands.

The Fourth Amendment requires "particularity" – specifically, that language in the warrant, or in supporting documents specifically incorporated by reference, "particularly describ[es] the *place to be searched, and the persons or things to be seized*." *See Groh v. Ramirez*, 540 US 551, 557 (2004) (emphasis added); *see also United States v. White*, 401 US 745, 758 (1971) ("wiretapping is a search and seizure within the meaning of the Fourth Amendment and therefore must meet its requirements," including particularity).

Underlying the particularity requirement in the Fourth Amendment is the abhorrence for"general warrants" and "writs of assistance," the language of which was so broad and vague as to grant practically unlimited discretion to authorities to search locations and seize people and things. *Steagald v. United States*, 451 US 204, 220 (1981) ("the general warrant specified only an offense" and "the writs of assistance . . . noted only the object of the search – any uncustomed goods"); *see also Boyd v. United States*, 116 U.S. 616, 625-30 (1886).

As the Ninth Circuit has explained, the purpose of the particularity

requirement, in addition to vindicating the staunch opposition to the practices of a tyrannical government, is to prevent "a general exploratory rummaging in a person's belongings." *United States v. Sears*, 411 F.3d 1124, 1127 (9th Cir. 2005), *quoting Coolidge v. New Hampshire*, 403 US 443, 467 (1971). In addition, as the Court in *Sears* elaborated, specificity in a warrant permits the individual who is the subject of the search and seizure to be "assure[d] . . . of the lawful authority of the executing officer, his need to search, and the limits of his power to search." *Id.*, *quoting United States v. Chadwick*, 433 US 1, 9 (1977).

In fact, the Ninth Circuit has held expressly that particularity in a warrant discourages confrontation between the officers and the individual searched, and ensures that the individual searched has the ability to prevent a violation by challenging any deviation from the authorized scope of the search and seizure. *Id.*, *citing Ramirez v. Butte-Silver Bow County*, 298 F.3d 1022, 1027 (9th Cir. 2002) (as amended).

In order for the particularity requirement to be met in the Ninth Circuit, "the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize." *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9th Cir. 1991). The detail necessary varies depending on "the particular circumstances and the nature of the evidence sought." *United States v. Adjani*, 452 F.3d 1140, 1147 (9th Cir. 2006).

For instance, descriptions of "generic categories of items" do not violate the Fourth Amendment when a "more precise description of the items subject to seizure is not possible." *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). But when descriptions are so imprecise that distinguishing between valid and invalid searches or seizures "require[s] police to exceed their expertise," warrants have been declared invalid for failing to meet the particularity requirement. *United States v. McLaughlin*, 851 F.2d 283, 286 (9th Cir. 1988).

When a warrant lacking in sufficient particularity has produced evidence used against an individual, the Ninth Circuit has adopted a "doctrine of severance," which permits the court to preserve the portions of the warrant untainted by the lack of

particularity, and suppress "[o]nly those articles seized pursuant to the invalid portions need be suppressed." *Sears*, 411 F.3d at 1129.

However, particularity is not met, and severability is not permissible, when "even the most specific descriptions . . . [were] fairly general and contained no time or subject matter limitations." *Sears*, 411 F.3d at 1130, *citing United States v. Cardwell*, 680 F.2d 75, 78–79 (9th Cir.1982). A complete failure to "specify any type of criminal activity or any type of evidence sought" would result in total suppression of evidence obtained pursuant to the warrant. *Id*., *citing United States v. McGrew*, 122 F.3d 847 (9th Cir. 1997).

Similar to the principle of particularity, a warrant must not be overbroad, requiring "that the scope of the warrant be limited by the probable cause on which the warrant is based." *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d at 856-57. Although many of the opinions in the Ninth Circuit have conflated the two requirements to some extent, the Court has clarified that the warrant's instructions, even if particularized, must also be "legal" in the sense that they are supported by "probable cause to seize the particular thing[s] named in the warrant." *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009).

The breadth requirement is a language requirement, similar to particularity, but which serves to ensure that searches and seizures do not extend beyond the scope of probable cause. *Spilotro*, 800 F.2d at 963 ("probable cause must exist to seize all the items of a particular type described in the warrant"). The breadth of a warrant limits the scope of search and seizure based on whether there is a "fair probability that contraband or evidence of a crime will be found in a particular place," not whether the language of the warrant is sufficiently specific to remove inappropriate discretion from the searcher's hands. *Id.* If the language of a warrant authorizes an official to exceed his legal authority (*i.e.*, to search and seize without probable cause), the warrant is invalid. *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d at 857, *citing Center Art Galleries- Hawaii, Inc. v. United States*, 875 F.2d 747 (9th Cir.1989) and *United States v. Washington*, 797 F.2d 1461, 1472 (9th Cir.1986).

3. *The Likely (and Separate) January 2008 Interception of Mr. Moalin's Electronic Communications Violated the Fourth Amendment*

The 3500 material related to the government's linguist (*see* Exhibit 6) demonstrates that Mr. Moalin's communications – in this instance, an incoming international telephone call – were intercepted not just via the dedicated FISA wiretap directed at his cellular telephone, but also concurrently, in real time, by "another agency's" independent means of interception.

For the reasons set forth in the analysis within Exhibit 7, that interception, too, lacked any of the elements and protections that would satisfy the Fourth Amendment, and is therefore invalid. Moreover, to the extent that interception was conducted pursuant to Section 702 (18 U.S.C. §1881a), Mr. Moalin was not provided the required notice. *See* **post**, at 24.

Thus, it appears that Mr. Moalin was subject to both of NSA's unlawful electronic surveillance programs, involving improper collection, storage, retrospective use, and interception of his electronic communications. Accordingly, Mr. Moalin renews his motion to dismiss the fruits of any such electronic surveillance, including that obtained from the FISA wiretap on his phone, and any evidence generated as a result. Also, in light of the government's failure to disclose to Mr. Moalin this other electronic surveillance, as well as the prospect that the FISA court was not apprised sufficiently of the background of the investigation, Mr. Moalin also renews his request for an evidentiary pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978)

II. *The Government Failed to Provide A Complete or Accurate Response to Mr. Moalin's Motion to Suppress the Electronic Surveillance (and Search) Conducted Against Him Pursuant to FISA*

The recent revelations regarding NSA collection and/or interception also raises the question whether the government – and that term is designed to include the government as a whole, including NSA– provided a complete or accurate response to Mr.

Moalin's motion to suppress the electronic surveillance conducted against him.[13]

Certainly the interception/collection conducted pursuant to Section 215 (50 U.S.C. §1861) was an indispensable factor in addressing the surveillance of Mr. Moalin's electronic communications. Yet the defense was not provided any notice of such interception/collection, or the role it played in the FISA process.[14]

In addition, the reference in the e-mail to Liban Abdirahman (the linguist) about "hear[ing] from another agency that Ayrow tried to call Basaaly today, but the call didn't go through[,]" (Exhibit 6 hereto), further demonstrates that the government's surveillance extended beyond ordinary FISA interception.

Also, as noted **ante**, in his pretrial motion to suppress, Mr. Moalin challenged any interceptions conducted pursuant to the FAA (50 U.S.C. §1881a), and to the extent any such interceptions occurred, they were subject to required notice to Mr. Moalin that was not provided. *See* 50 U.S.C. §1806(c), 1806(e) & 1881e(a).[15]

---

[13] On making this assertion counsel are not necessarily suggesting that it is the prosecutors in this case that are at fault here. In fact, it may well be the case that the NSA deliberately kept this information from the prosecutors as it did the public. *See, e.g.*, John Shiffman and Kristina Cooke, "U.S. Directs Agents to Cover Up Program Used to Investigate Americans," *Reuters*, August 5, 2013, available at http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805. The truth of the matter may well be that the NSA is deliberately misleading – if not outright lying – to the prosecutors. Particularly in light of these recent disclosures of abusive surveillance programs, Defendant's fair trial rights and rights to obtain exculpatory information should not be defeated by nuanced and one-sided statutory interpretation.

[14] To the extent such information was provided by the government to the Court *ex parte*, it merely underscores the need for disclosure to cleared counsel, *see* **post**, at POINT III, as defense counsel could have argued effectively the impact of that interception/collection on sufficiency and validity of the FISA application. It also would have enabled defense counsel to establish the exculpatory nature of the Section 215 interception/collection, and the need for discovery of the particulars involved in that interception/collection.

[15] In *Clapper v. Amnesty International USA*, ___ U.S. ___, ___, 133 S. Ct. 1138, 1154-55 (2013), one of the reasons urged by the government and adopted by

In the alternative, the Court should order discovery and conduct an evidentiary hearing to determine whether the government's response to Mr. Moalin's motion to suppress was complete and accurate.

III. *Cleared Defense Counsel Should Be Provided the Government's Response to Mr. Moalin's Motion to Suppress the Electronic Surveillance Pursuant to FISA, As Well As the Underlying FISA Applications, and Materials In Support Thereof, and the Court Should Revisit Its Review and Decisions with Respect to Any of the Government's Applications Made Pursuant to §4 of the Classified Information Procedures Act ("CIPA"), and Provide Those Submissions to Cleared Defense Counsel*

As noted **ante**, at 5-6, Mr. Moalin moved pretrial for disclosure of the FISA applications and supporting materials filed therewith. He also moved for disclosure of the government's CIPA §4 submissions, and the underlying material and information therein. The recent revelations about NSA surveillance, and the government's convenient and self-serving disclosure of the interception/collection related to Mr. Moalin – revealed not in the course of a criminal prosecution laden with Due Process protections and concurrent government obligations, but rather in the context of a calculated but clumsy attempt to justify the NSA programs in the wake of the political controversy revelation of their existence has generated – only reinforce the virtues of the adversary process, and the inherent and *practical* unfairness of a system that denies even cleared defense counsel the ability to advocate against the government's position.[16]

---

the Court to justify denying the plaintiffs in that case standing was because of the confidence that the statutory and constitutional validity of FAA surveillance would be adequately tested in the context of criminal prosecutions. Yet this case demonstrates that such confidence was misplaced, as the criminal process does not provide such opportunity in any genuine fashion, but instead merely repeats the secret, one-sided proceedings by which the authority for the surveillance was obtained.

[16] The Snowden NSA revelations have promoted the same adversarial concerns in the context of the FISA Court itself. *See* Spencer Ackerman, "US Senators Push for Special Privacy Advocate in Overhauled FISA Court", *The Guardian*, August 1, 2013, available at http://www.theguardian.com/law/2013/aug/01/fisa-court-bill-us-senate; Ezra Klein, "A Radical Plan for Shaking Up the FISA Court", *Washington Post*, July 9,

The law permits disclosure to defense counsel, yet not a single court has ever ordered such production. If this case does not present the situation in which such disclosure is not merely proper, but *necessary*, then §§1806(f) & (g) might as well not exist at all – and the same can be said for the adversary process, and defense counsel, as a whole. If cleared defense counsel cannot be afforded access to materials so essential to the case, and which shed light on the evidence, and the government's theory, in a manner otherwise hidden from the defense, what is the point of a lawyer for the defendant, for cross-examination, for a trial at all?

Under the circumstances, it cannot be suggested that Mr. Moalin has been provided his Sixth Amendment right to counsel, much less effective assistance thereof. Indeed, with respect to some of the most important issues in the case – that could categorically halt the prosecution altogether, or dramatically alter its evidentiary context – Mr. Moalin had, in reality, no lawyer at all.

This Memo of Law will not belabor the necessity of the adversary process in protecting the rights of the defendant, and in ultimately achieving justice as well as promoting confidence in the criminal justice system – *see* Docket #92, at 26-29, for an abbreviated treatment of the issue – but, as the Supreme Court recognized in *Alderman v. United States*, 394 U.S. 65 (1969) "[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate." *Id*., at 184; *see also Franks v. Delaware*, 438 U.S. 154, 169 (1978) (permitting adversarial proceeding on showing of intentional falsehood in warrant affidavit because the magistrate who approves a warrant *ex parte* "has no acquaintance with the information that may contradict the good faith and

---

2013, available at http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/09/a-radical-plan-for-shaking-up-the-fisa-court/.

reasonable basis of the affiant's allegations").[17]

In addition, while defense counsel have always been aware that they were operating at an insurmountable disadvantage by being denied access to the FISA applications or the underlying supporting documents (unlike any other situation in which the government seizes evidence pursuant to warrant), only recently has it been revealed that there exists a growing body of *law*, in the form of opinions by the Foreign Intelligence Surveillance Court ("FISC"), and the Foreign Intelligence Court of Review ("FISCR"), that are available to government counsel, but *not* to even cleared defense counsel.

Thus, unbeknownst to defense counsel, District Judge John D. Bates, Chief Judge of the FISC at the time, had issued an extraordinary opinion October 3, 2011, just before pretrial motions were filed in this case. Judge Bates excoriated NSA for exceeding its acquisition authority and making repeated misrepresentations to the FISC regarding NSA's activities during the very same time period in which Mr. Moalin's phone number was turned over to the FBI, and perhaps even when it was collected in the first place.

Judge Bates's language and concern is instructive for our own purposes here. For example, Judge Bates stated "[t]he court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation

---

[17] As the District Court in *United States v. Marzook*, 412 F. Supp.2d 913 (N.D. Ill. 2006), explained in the context of deciding whether to close a suppression hearing to the public because of the potential revelation of classified information thereat,

> [i]t is a matter of conjecture whether the court performs any real judicial function when it reviews classified documents in camera. Without the illumination provided by adversarial challenge and with no expertness in the field of national security, the court has no basis on which to test the accuracy of the government's claims.

Id., at 921, *quoting Stein v. Department of Justice & Federal Bureau of Investigation*, 662 F.2d 1245, 1259 (7th Cir. 1981).

regarding the scope of a major collection program." October 3, 2011, Memorandum Opinion, FISC, at 16 n. 14. A copy of the opinion is attached hereto as Exhibit 9.

While one example cited by Judge Bates is redacted,[18] another related to an NSA program that logged all domestic U.S. telephone calls. *Id*. Judge Bates also pointed out, referring to an earlier March 2009, FISC opinion (as yet undisclosed) that

> the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [REDACTED] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket [REDACTED]. Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not mee the required standard for querying. The Court concluded that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." *Id*.

Id. (Exhibit 9).

Judge Bates further noted that the government's submissions in that proceeding made it clear that NSA had been acquiring Internet transactions even before the FISC's first approval thereof, *id*., at 17, adding that:

- "for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different than what the Court had been led to believe." *Id*., at 28;
- "the Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCT's [multi-communication transactions], are consistent with the Fourth Amendment." *Id*., at 29;

---

[18] The publicly disclosed version – released in connection with a Freedom of Information Act lawsuit – is redacted, and is the only version defense counsel possess (or have seen).

- "NSA's minimization procedures, as the government proposes to apply them to MCT's as to which the 'active user' is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. §1881a(e) with respect to retention[.]" *Id*., at 80
- "[t]he sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of transactions is not feasible." *Id*., at 31;
- "the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications acquired or the extent to which those communications are to or from United States persons or persons in the United States." *Id*., at 31-32;
- "[e]ven if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection . . . it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future." *Id*., at 32;
- "the actual number of wholly domestic communications acquired may still be higher in view of NSA's inability conclusively to determine whether a significant portion of the MCT's within its sample contained wholly domestic communications." *Id*., at 34-35; and
- "the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year." *Id*., at 43.[19]

The repeated misrepresentations cited by Judge Bates in October 2011

[19] *See also* Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.," *The New York Times*, August 8, 2013, available at <http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all> (analyzing a document of internal NSA rules disclosed by Mr. Snowden).

are reminiscent of the FISC's 2002 opinion in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC), *rev'd on other grounds sub nom.*, *In re Sealed Case*, 310 F.3d 717 (FISCR 2002),[20] in which the FISC, in its first opinion ever, reported that beginning in March 2000, the Department of Justice (hereinafter "DoJ") had come "forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts," including:

- "75 FISA applications related to major terrorist attacks directed against the United States" contained "misstatements and omissions of material facts." 218 F. Supp. 2d at 620-21;
- the government's failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance. *Id*.; and
- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id*.

According to the FISC, "[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . ." *Id*., at 621. Nor were those problems isolated or resolved by those revelations. Instead, they proved persistent. A report issued March 8, 2006, by the DoJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other intelligence-gathering procedures more than 100 times in the preceding two years, and problems appear to have grown more frequent in some crucial respects. *See* Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March 8, 2006 (hereinafter "DoJ IG Report"), available at http://www.usdoj.gov/oig/special/s0603/final.pdf.

The report characterized some violations as "significant," including wiretaps that were much broader in scope than authorized by a court ("over-collection"), and others

[20] "FISCR" refers to the Foreign Intelligence Court of Review, which is the appellate court for the FISC, and is comprised of three federal Circuit judges. The FISCR's 2002 decision in *In re Sealed Case* marked its first case since enactment of FISA in 1978.

that continued for weeks and months longer than authorized ("overruns"). *Id*., at 24-25.[21] FISA-related overcollection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. *See* DoJ IG Report, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, *id*., at 29, although the amount of time "over-collection" and "overruns" were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id*., at 25.

The lack of veracity catalogued in these two opinions is inevitable in a system in which there is no opponent to dispute facts or hold opponents accountable for misrepresenting facts, and in which the court lacks investigative authority or any practical, meaningful means of oversight over the collection/storage/interception process. Indeed, an internal May 2012 audit of NSA's surveillance programs – among the documents recently disclosed by Mr. Snowden – found that NSA violated privacy rules protecting domestic U.S. communications 2,776 times in a one-year period. *See SID Oversight & Compliance*, Quarterly Report, First Quarter Calendar Year 2012, May 3, 2012, available at <http://www.documentcloud.org/documents/758651-1qcy12-violations.html#document/p12>.

Unfortunately, in a system in which NSA and other intelligence organs are free to misrepresent without challenge or accountability, little has changed except perhaps NSA's enhanced dexterity in abusing and manipulating the FISC and the FISA system as a whole.

Defense counsel have always believed that contesting a motion without access to the facts is untenable, but denial to both the facts *and* the law is unconscionable.

---

[21] The DoJ Inspector General's report was not instigated by the government itself. Rather, the publication of documents released to Electronic Privacy Information Center (hereinafter "EPIC") in Freedom of Information Act litigation prompted the DoJ IG to use those and other documents as a basis for the report. In preparing the report the IG reviewed only those 108 instances in which the FBI itself reported violations to the Intelligence Oversight Board – a four-member Executive Branch body that ordinarily does *not* submit its reports to Congress.

As a result of this vertical playing field, with the government at the apex and the defense at the bottom, a criminal defendant and his counsel are compelled to operate in a system in which the admissibility of evidence at the core of the government's case – in this case, in effect the *entirety* of the government's case – is decided on the basis of a secret body of facts *and* law to which even cleared defense counsel is denied access.[22]

The unfairness of such a system is manifested in the government's perfect record in FISA and CIPA §4 litigation. Being in complete and unilateral control of the contents of the facts and the law, is it any wonder that the government has prevailed each and every time? Such a system does not provide Due Process, or even approach it. If a U.S. citizen charged in another country were to be subjected to such a system, it would be the subject of bipartisan nationwide opprobrium. Yet it is not any more acceptable because it is happening here; instead, it is *less* tolerable.[23]

Thus, this case presents the manifest unfairness in which key evidence relating to the core of the government's case was withheld from the defense in the context of both the legal determination whether such evidence was obtained legitimately, as well as the factual context, in which the evidence fatally undercut the linchpin of the government's theory at trial.

---

[22] That embargo on such important information and material renders defense counsel's security clearance entirely ineffectual, as it is not a factor with respect to gaining access to information essential to perhaps the critical legal and factual determination in the case.

[23] Regarding the FISC's *ex parte* proceedings, *The New York Times* reported that Geoffrey R. Stone, professor of constitutional law at the University of Chicago, "said he was troubled by the idea that the court is creating a significant body of law without hearing from anyone outside the government, forgoing the adversarial system that is a staple of the American justice system. 'That whole notion is missing in this process,' he said." Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *The New York Times*, July 6, 2013, available at <http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all>.

Accordingly, it is respectfully submitted that the Court should order disclosure to cleared defense counsel the FISA applications and supporting materials, as well as the government's CIPA §4 submissions and underlying related documents, and revisit its CIPA §4 decisions with full participation by defense counsel consistent with the principles of the adversary system.[24]

IV. *The Government Failed to Provide Necessary Rule 16 Discovery*

The recent revelations regarding NSA collection and/or interception establishes that the government – and again that term is designed to include the government as a whole, including NSA – provided a complete or accurate response to Mr. Moalin's motion to suppress the electronic surveillance conducted against him.

In addition, the reference in the January 24, 2008, e-mail to Liban Abdirahman (the government's Somali linguist), from a redacted source (probably SA Michael C. Kaiser, the FBI case agent) that states, "We just heard from another agency that Ayrow tried to call Basaaly today, but the call didn't go through[,]" (Exhibit 6 hereto), further demonstrates that the government's surveillance extended beyond ordinary FISA interception.

Yet neither of those interceptions and/or collection of Mr. Moalin's communications, or data related thereto, was provided to Mr. Moalin as part of Rule 16 discovery, even though they clearly are covered by Rule 16's disclosure obligations. For example, it is axiomatic that any items seized from the defendant, by any means, are discoverable. *See* Rule 16(a)(1)(E)(iii) (government must permit inspection of items if they were "obtained from or belong[] to the defendant"). In addition, Rule 16 also requires discovery of items "material to preparation of the defense." Rule 16(a)(1)(E)(i).

Also, here, the interception/seizure of his electronic communications, and data related thereto, constituted a seizure just as it would in the Title III context. *See* 18

---

[24] *See* Hon. James G. Carr, Op-Ed, "A Better Secret Court," *The New York Times*, July 23, 2013, available at <http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html?ref=opinion&_r=1&>.

U.S.C. §2518 (8)(d) & (9). The notion that such records obtained via either Section 215 (§1861) or Section 702 (§1881) would or could be immune from discovery is simply without precedent or foundation.

Even if the government were to rely on CIPA §4 or Rule 16(d)(1) as a means of avoiding production, the exculpatory character of the interceptions or data (as explained **ante** in POINT III) would make them discoverable under both sections. Moreover, to the extent such vital information and materials were addressed in the government's CIPA §4 application(s), that merely highlights the complete unfairness – and denial of Due Process – in denying cleared defense counsel access to such applications and the underlying information the government sought to exempt from discovery.

Also, the government cannot argue that the interception/collection was not related to this case (which might enable it to be non-discoverable under Rule 16 or CIPA §4). Here, the information and material go to the basis for the government's investigation, and the heart of its theory at trial, namely, whether Mr. Moalin was communicating directly with Aden Ayrow. For the same reason, and also because of their dubious legality, any "programmatic analytics" are also discoverable and should have been (and should now be) produced.

At the very least, production of that material and information would have enabled the defense to examine the telephone numbers Mr. Moalin called (or which called him), identify them, conduct an investigation, and use those results in cross-examination or the defense case (through either or both documents and witnesses).

As a result, it is respectfully submitted that the government's failure to discharge its Rule 16 obligations require a new trial, or, at the very least, disclosure of the information and material in question, and an evidentiary hearing.

V. ***Congressional Testimony and Other Statements By FBI and NSA Officials Have Fatally Undermined Not Only the Essential Element of the Government's Theory at Trial, But Also Public Confidence In the Investigation and Prosecution of This Case***

As set forth **ante**, at 3, 4-5, the government based its case on trial on the assertion that Mr. Moalin was in direct communication with Aden Ayrow: that the "Sheikalow" on the intercepted telephone conversations was, in fact, Mr. Ayrow. Yet Deputy Director Joyce's admission that the contact Mr. Moalin had with a terrorist organization that instigated the second investigation of Mr. Moalin was *in*direct casts serious doubt on that position.

That raises at least the following critical questions:

1. was that *in*direct contact to the same telephone number(s) used by "Sheikalow," which would establish that even the government did not believe "Sheikalow" was Mr. Ayrow himself? and
2. was that *in*direct contact the same person as "Sheikalow," and therefore not Mr. Ayrow?
3. whose telephone number was it, and how was that person identified (and how was he deemed "connected" to a terrorist organization?

Either way, the concession of *in*direct contact during the relevant time period – rather than *direct* contact with Mr. Ayrow – fatally undermines the government's theory. In addition, the impact of the linguist's 3500 material is equally profound:

1. how did the other U.S. government agency know it was *Mr. Ayrow* who was attempting to contact Mr. Moalin in January 2008?
2. did that agency have Mr. Ayrow's telephone number?
3. was it different than the number(s) used by "Sheikalow"?
4. what was the number used by Mr. Ayrow during that intercepted attempted call?

Again, the information underlying that 3500 material could very well have torpedoed the government's theory entirely, and regardless of the answers, the government's failure to provide the defense with the information is indefensible and

inexcusable.

In addition, the manner in which Mr. Moalin remained – perhaps forever – on the government's radar, leading to this investigation, has dramatically eroded public confidence in the fundamental fairness of the investigation and prosecution of this case, and its use as a justification for the most massive electronic surveillance, collection, storage, and interception programs in human history. *See, e.g.,* Max Fisher, "Is This $8,500 Wire Transfer Really the NSA's Best Case for Tracking Americans' Phone Records?" *The Washington Post*, August 9, 2013, available at <latimes.com/news/politics/la-pn-secret-nsa-surveillance-court-order-20130731,0,1310703.story>; Ken Dilanian, "Public Gets First Look At Once-Secret Court Order on NSA Surveillance," *Los Angeles Times*, July 31, 2013, available at http://articles.latimes.com/2013/jul/31/news/la-pn-secret-nsa-surveillance-court-order-20130731 ("officials remained unable to come up with more than one relatively minor terrorism-financing case in which the phone records had proved instrumental").[25]

Accordingly, it is respectfully submitted that the Court should grant defendants a new trial, order the government to disclose the underlying materials, and conduct the appropriate evidentiary hearings regarding the role of NSA, its use of the FAA and other surveillance programs, including Section 215 (50 U.S.C. §1861) in the investigation and prosecution of this case.

---

[25] The sanitizing of the origins of criminal investigations has already leached from the national security sphere and is poised to contaminate a much wider type of ordinary criminal prosecution, and involves concealment from not just the defense. *See, e.g.,* Shiffman and Cooke, "U.S. Directs Agents to Cover Up Program Used to Investigate Americans," *Reuters*, August 5, 2013, available at <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805> ("[a]lthough these case rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges").

VI. *The Government Failed to Provide Mr. Moalin Exculpatory Material and Information*

Requests for *Brady* material often occur in a partial vacuum: because the government possesses the information and materials, more often than not defendants can only propose subject matters of exculpatory material and information that might exist without firm knowledge of whether it, or in what form, it exists at all.

As a result, courts, too, are not usually in a position to identify exculpatory material and information with precision, and instead are limited to reminding the government of its obligation to provide *Brady* material, and deferring to the government's recognition of that duty.

However, here, defendants and the Court are now aware of specific *Brady* material that exists, but which the government did not produce, namely, the Section 215 interception/collection and the underlying information related to the previously terminated investigation of Mr. Moalin (that likely contributed to the conclusions noted in the FIG Assessment).

While still unable to identify the exact form in which such exculpatory material and information exists, defendants can now to some extent articulate its nature:

(a) the reasons underlying the conclusion, at the end of the initial post-9/11 investigation of Mr. Moalin, that he was not engaged in illegal conduct or linked to terrorism. Also, that earlier investigation likely yielded abundant if not conclusive evidence that Mr. Moalin was sending money to Somalia for humanitarian and other (family) purposes even before *al Shabaab* existed, and that he did not harbor anti-U.S. or pro-terrorist sympathies;[26]

(b) evidence that Mr. Moalin's contacts with *al Shabaab* that precipitated renewal of the investigation were *in*direct, and not directly with Mr.

[26] The FIG Assessment (Exhibit 1) was prepared in April 2009, while the initial investigation occurred years earlier (2003). As a result, the information from either might be in many ways distinct.

Ayrow;

(c) anything exculpatory generated by and during the earlier Anaheim investigation referred to in Ahmed Nasir's PSR in which no charges were ever filed against Nasir; [27] and

(d) exculpatory information and material related to the FIG Assessment itself, which Mr. Moalin requested in his pretrial motions.

Of course, the government's production – and its search for such materials and information – should not be limited to the items enumerated above, but should also include any other exculpatory material and information reviewed in the process (as the defense is still for the most part in a position of *not* knowing the specific nature and type of exculpatory information and material in the government's possession).

Conclusion

For all the reasons set forth above, and in all papers previously submitted in this case, it is respectfully submitted that the Court should grant defendants' Rule 33 motion, and order anew trial, and/or compel the discovery demanded in this motion, and/or conduct the evidentiary hearings requested herein.

Dated: 5 September 2013
New York, New York

Respectfully submitted,

S/ Joshua L. Dratel
JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, NY 10006

Attorneys for Basaaly Moalin

S/ Linda Moreno
LINDA MORENO
Linda Moreno, P.A.
PO Box 10985

[27] Mr. Ahmed Nasir's PSR notes that the "case agent advised [the Probation Officer] that the defendant was originally investigated in Anaheim, California, prior to his known connections in this offense."

Tampa, Florida 33679

Attorney for Mohamed Mohamud

S/ Ahmed Ghappour
AHMED GHAPPOUR
The Law Offices of Ahmed Ghappour
PO Box 20367
Seattle, Washington 98102

Attorney for Issa Doreh

S/ Thomas A. Durkin
THOMAS A. DURKIN
Durkin & Roberts
Attorneys and Counselors
2446 North Clark Street
Chicago, Illinois 60614

Attorneys for Ahmed Nasir Taalil Mohamud