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: November 13, 2013 Time: 1:30 p.m. REPLY TO GOVERNMENT'S OPPOSITION TO DEFENDANTS' 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 Reply Memorandum of Law is submitted on behalf of defendant Basaaly Moalin and his co-defendants, Mohamed Mohamed Mohamud, Issa Doreh, and Ahmed Nasir Taalil Mohamed, in response to the government's Memo of Law in Opposition to defendants' motion, pursuant to Rule 33, Fed.R.Crim.P., for a new trial. Much of the government's response in opposition was anticipated and addressed in Mr. Moalin's initial Memo of Law, and/or does not require rejoinder. Thus, this Reply will concentrate on specific facets of the government's opposition.

The government's Memo of Law – or at least that modest portion that is not redacted, and which defense counsel and the public can therefore review – is noteworthy not only for what it asserts, but also what it fails to address. In seeking to avoid any accountability for its heretofore unacknowledged interception, collection, and/or retention of Mr. Moalin's electronic communications, or any inquiry whether it was conducted lawfully or constitutionally, the government would freeze the legal and technological analysis in the era of rotary dial phones and discrete manual land line interception.

The government relies on authority that is not only antiquated and completely overwhelmed by technological development, but also on authority from a court, the Foreign Intelligence Surveillance Court (hereinafter "FISC"), that meets in secret, hears from only one side, and issues secret opinions – resulting in, unsurprisingly, and inexorably as B follows A, a forum in which the government always wins despite the continued series of lies fed it by the National Security Agency (hereinafter "NSA") with respect to the scope and implementation of its interception, collection, and retention programs.

Indeed, while the FISC has repeatedly caught NSA in material prevarications that affect the very programs at issue in this case, the FISC, treating NSA like the favored child a parent is unwilling to discipline, merely wags it finger yet inevitably yields to NSA the authority to construct the most massive, pervasive, and unfettered surveillance state in history without any genuine or meaningful supervision.

Also, astonishingly, in defending its interception, collection, and/or retention of Mr. Moalin's electronic communications at issue in this motion, the government fails to *mention at all*, much less confront, the series of recent Supreme Court decisions that have integrated fundamental privacy interests and technological advances into a modern and functional Fourth Amendment jurisprudence, and which have, in the course of doing so, explicitly presaged re-evaluation of the outdated and insufficient "third party records" doctrine upon which the government stakes its entire argument.

In that context, Mr. Moalin's privacy interests are manifest and cognizable, protected and enforceable. At the very least, a fresh, independent approach to the issue is a necessity both as a matter of doctrinal legal analysis as well as constitutional imperative.

In addition, the government continues to resist at all costs any authentic examination of the communications it has intercepted, collected, and/or retained, the manner in which it has done so, the use it has made of that information, and its impact upon the admissibility of its evidence in this case and the ultimate result at trial. Moreover, the continued extensive redactions in the government's papers demonstrate that relevant, material, and/or exculpatory information – either factual or legal, or both – is being withheld from cleared defense counsel because, if the government's technical legal arguments are meritorious, and/or the NSA's interception/collection/retention programs are not at issue in this case, a simple "no" would suffice.

Yet, at some point, though, an Article III court, in an Article III proceeding, must decide these issues in a manner consistent with the requirements of Article III and the Constitution – including fully adversary proceedings that lie at the core of the accuracy, reliability, and integrity of a criminal justice system's adjudications. This motion provides the perfect opportunity for such a determination, rather than the continued pretense that a one-sided process in which one side uses secret facts and law as both a sword and shield can ever adequately inform a court, or provide a defendant a legitimate chance to prevail.

This motion is of profound importance, not only to Mr. Moalin – who, as an adolescent refugee from a ravaged conflict zone who grew up to be a gainfully employed

U.S. citizen productive in his community, serves as a paradigmatic example of American aspirations in both idealized and practical terms – but also to the criminal justice system's commitment to afford due process to each defendant regardless of the offense charged, and regardless of the government's unilateral opinion as to what is relevant to the legal and factual determinations a court must make in the process.

As Sixth Circuit Judge Damon J. Keith – who was the District Court judge in the case that resulted in the Supreme Court's historic opinion in *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972) – wrote in *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 683 (6th Cir. 2002), "Democracies die behind closed doors." Here, the government seeks to keep the door closed not only on the illegality of the methods by which it obtained information and evidence against Mr. Moalin, but also the very means by which the question itself is to be adjudicated. Marshaling a body of secret laws and secret facts behind that closed door, the government has placed the values of democracy – as they are reflected in the operation of the criminal justice system – on life support, and is ready to pull the plug.

This Court is in a unique and constitutionally authorized position to prevent that, and instead vindicate those of Mr. Moalin's rights that are at stake here, including those guaranteed by the Fourth, Fifth, First, and Sixth Amendments. Accordingly, it is respectfully submitted that the Court should grant Mr. Moalin's Rule 33 motion in its entirety.

ARGUMENT

A. *The Government's Collection of Mr. Moalin's Telephony Metadata Violated His Constitutional Rights Under Both the Fourth and First Amendments*

The government's defense of NSA's interception, collection, and retention of Mr. Moalin's electronic communications – at least in the form of telephony metadata, but perhaps more – is premised upon two unavailing bases: (1) the "third party records" doctrine, and in particular the decision in *Smith v. Maryland*, 442 U.S. 735 (1979); and (2) decisions of the FISC, a court that convenes secretly, that hears only from the government,

and which has never placed a substantive brake on the NSA's electronic surveillance programs.[1]

1. *Mr. Moalin Possesses a Legitimate and Cognizable Expectation of Privacy In His Telephony Metadata*

In hewing to *Smith v. Maryland*, the government ignores *completely* a series of recent Supreme Court opinions that have rendered *Smith* – decided in a limited, technologically simplistic context involving a single defendant whose single phone line was monitored to identify the numbers called and calling (a pen register) – entirely obsolete and inapplicable.

Recognizing the impact of modern data collection capabilities, and the uses to which they can be put, the Court has modernized the applicable Fourth Amendment jurisprudence. As a result, the notion that the Fourth Amendment's protection against unreasonable searches and seizures does not extend to third party records because knowingly exposing information to third parties negates any expectation that the information will remain private, even with assurances that it will be kept confidential, is no longer viable.

---

[1] In this pleading, as in Mr. Moalin's Initial Memo of Law, the conventional use of "government" to describe the prosecutors does not apply. Rather, the "government" denotes a much broader and remote set of agencies, including, specifically, those involved in gathering intelligence. Sufficient evidence exists in the public domain to question whether those intelligence-gathering agencies are honest with members of the United States Attorney's Office, or the Department of Justice, or other elements not within some narrow intelligence-gathering umbrella. *See, e.g.*, John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/15xWJwH (in the context of "parallel construction" [discussed **post**, at 16], describing agent's effort to conceal from prosecutors the origins of a tip); Ruth Marcus, "James Clapper's 'least untruthful' answer," *Washington Post*, June 13, 2013, (available at http://articles.washingtonpost.com/2013-06-13/opinions/39950057_1_oversight-national-intelligence-national-security-agency)(describing how James Clapper, Director of National Intelligence, stated how he answered questions posed by Senator Ron Wyden in the "least untruthful manner").

For example, most recently, in in *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2012) (Sotomayor, J., concurring), Justice Sotomayor recognized that the current approach to the concept of privacy, which essentially requires absolute secrecy to trigger Fourth Amendment protections, is "ill suited to the digital age." *Id*., at 957. By opening the door to reevaluating the third party records doctrine, Justice Sotomayor has placed courts on notice that the changes wrought by developing technology must be incorporated in Fourth Amendment analysis.

As Justice Sotomayor explained in *Jones*,

> [m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g.*, *Smith*, 442 U.S. at 742, *United States v. Miller*, 425 U.S. 435, 443 (1976) . . . People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Id.

In fact, Justice Sotomayor's observation that the doctrine might be too blunt an instrument in current times echoes other Supreme Court opinions that have recognized that the expectation of privacy remains intact despite the possibility that third parties have access to certain information. *See e.g. Florida v. Jardines*, ___ U.S. ___, 133 S. Ct. 1409 (2013) (odors detectable by a police dog that emanate outside of a home); *Kyllo v. United States*, 533 U.S. 27 (2001) (thermal signatures emanating from a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results held by hospital staff).

The government's failure even to mention these cases, much less address them, in tandem with its reflexive reliance on *Smith*, is akin to a 16th century mariner utilizing nautical charts prepared by those still insisting the world was flat instead of charts provided by Columbus upon his return from the New World.

Indeed, given the advances in technology since *Smith*, and the impact those developments have had on the expectation of privacy, the NSA's collection/retention of telephony metadata clearly qualifies for Fourth Amendment protection. A Fourth Amendment search occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo*, 533 U.S. at 33.

Judged pursuant to that standard, the long-term recording and aggregation of telephony metadata constitutes a search. Mr. Moalin would not expect that the government will make a note, every time he picks up the phone, of whom he calls, precisely when he calls them, and for precisely how long they speak. Nor should he have to do so. *See, e.g.*, *United States v. Gordon*, 236 F.2d 916, 919 (2d Cir. 1956); Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1934 (2013) (until recently, "the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states").[2]

Moreover, the expectation that telephony metadata will not be subjected to long-term recording and aggregation by the government is objectively reasonable. The kind of surveillance at issue here provides the government a comprehensive record of associations, revealing a wealth of detail about familial, political, professional, religious, and intimate relationships – the same kind of information that could traditionally be obtained only by examining the contents of communications.

Aggregating metadata over time can yield an even richer repository of personal and associational details than content, and obliterates any controlling value

---

[2] *See also* Danielle Keats Citron and David Gray, "Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards," 126 Harv. L. Rev. F. 262 (May 2013) (reviewing Fourth Amendment jurisprudence post-*Jones* and addressing more the dangers of allowing pre-existing Fourth Amendment principles to control analysis in the current age of electronic surveillance).

the narrow context in *Smith* might supply. Here, the duration of surveillance results in law enforcement being able to "stitch together an intimate portrait of [a person's] daily life based on information that one would reasonably expect to remain private." "Electronic Surveillance & Government Access to Third Party Records," *National Association of Criminal Defense Lawyers*, February 19, 2012, available at <http://www.nacdl.org/reports/thirdpartyrecords/thirdpartyrecords_pdf/>.

Technology has altered the concept of privacy, and demonstrated that the amount of information collected, either in type or duration, even if it is seemingly harmless in isolation, can change the character of the search under the Fourth Amendment. *See* Jim Harper, "Escaping Fourth Amendment Doctrine After *Jones*: Physics, Law and Privacy Protection," *Cato Supreme Court Review*, available at <http://www.cato.org/sites/cato.org /files/serials/files/supreme-court-review/2012/9/scr-2012-harper.pdf.>

In that essay, Mr. Harper outlines the "mosaic theory" of privacy, explaining the D. C. Circuit's finding that the GPS tracking of the defendant in *Jones*, which continued for 28 days, was different in character from the traditional idea of "exposing" information to the public:

> "Exposure," it found, is based on ''not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do.'' The court held that ''the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil.'' Under this reasoning, Jones's movements were not actually ''exposed.'' [Additionally] the court wrote that the whole of one's movements over the course of a month ''reveals far more than the individual movements it comprises. The difference is not one of degree but of kind.''

Id. at 223.[3]

[3] The August 2012 issue of the *ABA Journal* presented both sides of the argument in "The Data Question: Should the Third-Party Records Doctrine Be

That analysis, resonating in Justice Sotomayor's concurrence in *Jones*, accounts for the fact that non-content information, when collected in bulk, has the potential to invade privacy as much as collection of content information. Thus, the surveillance at issue here achieves essentially the same kind of privacy intrusion that led five Justices to conclude in *Jones* that the long-term recording and aggregation of location information constituted a search.

In *Jones*, the Court considered whether police had conducted a Fourth Amendment search by attaching a GPS-tracking device to a vehicle and monitoring its movements over a 28-day period. The Court held that the installation of the GPS device and the use of it to monitor the vehicle's movements constituted a search because it involved a trespass "conjoined with . . . an attempt to find something or to obtain information." *Id*. at 951 n.5.

In two concurring opinions, five Justices concluded that the surveillance constituted a search because it "impinge[d] on expectations of privacy." *Id*. at 964 (Alito, J., concurring); *id*. at 955–56 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . ."); *id*. at 955 (individuals possess "a reasonable societal expectation of privacy in the sum of [their] public movements.").

What Justice Sotomayor observed of long-term location tracking is equally true of the mass call-tracking program encompassed by Section 215 (50 U.S.C. §1861). Indeed, the program is in several respects considerably *more* intrusive than the location tracking that was at issue in *Jones*. That case involved the surveillance of a single vehicle for 28 days. The mass call-tracking program, by

---

Revisited?", available at <http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/>. *See also* Jennifer Granick, "Debate: Metadata and the Fourth Amendment," September 23, 2013, available at <http://justsecurity.org/2013/09/23/metadata-fourth-amendment/>.

contrast, has involved broad and indiscriminate electronic surveillance and collection/retention of that surveillance of every American over a period of years, and which the government appears intent on continuing indefinitely.

Similarly, nothing in *Smith* remotely suggests that the Constitution permits the indefinite collection of sensitive information about every single phone call made or received by those inside the U.S. In *Smith*, the Supreme Court upheld the installation of a "pen register" in a criminal investigation. The pen register in *Smith*, however, was primitive – it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls. *Id*., at 741. It was in place for fewer than two days, and it was directed at a single criminal suspect. *Id.* at 737. Moreover, the information the pen register yielded was not aggregated with information from other pen registers, let alone with information relating to hundreds of millions of innocent people, and available for an indeterminate period in the future. *Id*. *See also* David Kravets, "How a Purse Snatching Led to the Legal Justification for NSA Domestic Spying," *Wired.com*, October 2, 2013, available at <http://www.wired.com/threatlevel/2013/10/nsa-smith-purse-snatching/>.

Thus, *Smith* itself, in addition to *Jones*, *Kyllo*, and *Jardines*, confirms that an individual's expectation of privacy in information does not hinge simply on whether he has shared it with another person. Otherwise, even the *contents* of phone calls or e-mail would be constitutionally unprotected, as both are shared with third parties.

Nor could a decision by the FISC, cited by the government, in its Memo of Law, at 15 [*In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, 2013 WL 5307991, at *5 (FISC August 29, 2013)], change that conclusion, particularly since that FISC opinion, too, fails to confront *Jones* or its kindred cases. In fact, citation to that decision is the type of unsurprising bootstrapping that secret, one-party proceedings can produce

with respect to judicial opinions in which only one party gets to contribute any legal analysis.[4]

Nor was NSA's interception/collection/retention of Mr. Moalin's telephony metadata "reasonable" for purposes of Fourth Amendment analysis. As the Supreme Court has explained, "the ultimate touchstone of the Fourth Amendment" is "reasonableness[.]" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Reasonableness is determined by examining the "totality of circumstances" to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169 (2008).

In the context of electronic surveillance, reasonableness demands that statutes have "precise and discriminate" requirements and that the government's surveillance authority be "carefully circumscribed so as to prevent unauthorized invasions of privacy." *Berger v. New York*, 388 U.S. 41, 58 (1967) (quotation marks omitted). Here, as applied to Mr. Moalin, Section 215's suspicionless, indefinite, and unduly broad character fails that analysis entirely.

Section 215's mass call-tracking program also violated Mr. Moalin's Fourth Amendment rights because it authorized warrantless searches, which "are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967); *see United States v. Karo*, 468 U.S. 705, 717 (1984). In fact, the

---

[4] Another eminently frustrating aspect of the government's refusal to engage on these issues is manifested in the footnote to citation of that FISC opinion, which footnote *is redacted* from the government's Memo of Law. Counsel cannot be effective advocates, consistent with their constitutional and ethical obligations, when they are deprived not only of the facts, but also the law, on an issue material to a client's litigation.

program authorizes the particular form of search that the authors of the Fourth Amendment found most offensive; in effect, the program constitutes a general warrant for the digital age. *See Berger*, 388 U.S. at 59.

Also, Courts have insisted that the government's intrusions on privacy be precise and discriminate. *See Berger*, 388 U.S. at 58. The mass call-tracking program is anything but, and in pursuit of its limited objective of tracking the associations of a discrete number of individuals, the government has employed the most indiscriminate means possible – collecting *everyone's* records. The government has, in the words of Section 215's author, "scoop[ed] up the entire ocean to . . . catch a fish." Jennifer Valentino-Devries & Siobhan Gorman, "Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering," *The Wall Street Journal*, July 8, 2013, http://on.wsj.com/14N9j6j (quoting Rep. Jim Sensenbrenner).

2. *Mr. Moalin Possesses the Requisite Standing to Challenge the Government's Collection of His Telephony Metadata*

The government's claim that Mr. Moalin lacks standing to challenge the NSA's interception/collection/retention of his telephony metadata is based on its invocation of *Smith*, which, as noted above, is unavailing.

Also, in a civil lawsuit, *ACLU, et al. v. Clapper*, 13 Civ. 03994 (WHP) (S.D.N.Y.), the government has acknowledged that NSA has "examined" a person's call records when, after NSA upon querying its database, links that person to a targeted telephone number. *See* Defendant's Memorandum of Law in Support of Motion to Dismiss (Dkt. #33), at 32-33. That appears to be precisely what occurred here with respect to Mr. Moalin. *See* Mr. Moalin's Initial Memo of Law, at 19-20.

The government's remaining objection to standing emanates from the FISC's opinion cited **ante**, which does not even account for the principal Supreme Court cases and cannot be controlling on a court required to hear from both parties to litigation, and whose opinions are subject to public review and appeal.

Also, the Foreign Intelligence Surveillance Act (hereinafter "FISA") authorizes "an aggrieved person" [*see* 50 U.S.C. §§1801(k) & 1821(2)] to seek

suppression any evidence derived from FISA surveillance or searches on grounds that (1) the evidence was unlawfully acquired, or (2) the electronic surveillance or physical search was not conducted in conformity with the order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f).

To the extent NSA's conclusion that Mr. Moalin had indirect contact with an extremist outside of the U.S. was a result of an evaluative analysis conducted on a database containing data *exclusively* obtained under Section 215 (whether the result of a manual or "automated query program") the metadata from which NSA inferred Moalin's alleged "indirect" contact with a known terrorist was most probably "third hop" metadata, meaning that Mr. Moalin could have been in contact with a person A, who was in contact with another person B, who was, in turn, in contact with a "known terrorist." This, alone, could not have been sufficient to satisfy FISA's probable cause requirements, and would also have, given the ultimate conclusion that Mr. Moalin was not connected to terrorist activity, involved interception/collection/retention in violation of the First Amendment (and FISA's prohibitions on investigating the First Amendment activities of U.S. persons).

Conversely, to the extent the NSA's conclusion (regarding Mr. Moalin) was acquired or derived from a "contact-chain," the Court should evaluate the "foreign intelligence justification" used to justify the commencement of, or query within, the chain to ensure it satisfied the language, purpose and intent of the FISA statute.

In that context, the 215 Bulk Primary Order orders that the FISA "Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata." This tradecraft without doubt includes evaluative analytics *across all databases in the NSA*. Thus, to the extent NSA's conclusion (that Mr. Moalin had indirect contact with an extremist outside of the U.S.) was a result of evaluative analysis conducted on a database consisting of a *combination* of data acquired under Section 215, Section 702 and/or alternative methods of collection such as Executive Order 12333.

(whether the result of a manual or "automated query program") the Court should suppress because the FISA 702 evidence was unlawfully acquired (for reasons stated **ante** and in Mr. Moalin's Initial Memo of Law).

Such "tradecraft" without doubt would also include verification and/or confirmation analytics *across all databases in the NSA*. Thus, to the extent that the NSA's conclusion (that Mr. Moalin had indirect contact with an extremist outside of the U.S.) was *confirmed or verified* by information acquired or derived from Section 702 surveillance and/or alternative methods of collection such as Executive Order 12333, was a result of evaluative analysis conducted on a database consisting of a *combination* of data acquired under Section 215, Section 702 and/or alternative methods of collection such as Executive Order 12333 (whether the result of a manual or "automated query program"), the Court should suppress because the FISA 702 evidence was unlawfully acquired.

3. *The NSA's Collection and Retention of Mr. Moalin's Telephony Metadata Violated His First Amendment Rights*

Contrary to the government's assertion, in its Memo of Law, at 17 n. 9, Mr. Moalin does indeed possess First Amendment rights that were violated by NSA's interception, collection, and/or retention of his telephony metadata pursuant to Section 215.

Courts have repeatedly recognized that the government's investigatory and surveillance activities can infringe on rights protected by the First Amendment – and that the First Amendment has force independent of the Fourth Amendment. *See, e.g.*, *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963); *Tabbaa v. Chertoff*, 509 F.3d 89, 102–03 & n. 4 (2d Cir. 2007); *FEC v. LaRouche Campaign, Inc.*, 817 F.2d 233, 234-35 (2d Cir. 1987); *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Commissioner of New York Harbor*, 667 F.2d 267, 269 (2d Cir. 1981).

In particular, courts apply "exacting scrutiny" when investigatory tools substantially burden First Amendment rights. *In re Grand Jury Proceedings*, 776

F.2d 1099, 1102–03 (2d Cir. 1985) (grand-jury subpoena); *Clark v. Library of Cong.*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *Nat'l Commodity & Barter Ass'n v. Archer*, 31 F.3d 1521, 1531 n. 4 (10th Cir. 1994) (seizure of organization's membership information).

Nor do the First Amendment's protections vanish simply because investigative activities also implicate or even satisfy the Fourth Amendment. The interests guarded by these rights are distinct. *See Tabbaa*, 509 F.3d at 102–03 n. 4; *Ealy v. Littlejohn*, 569 F.2d 219, 227 (5th Cir. 1978) ("[w]e therefore conclude that the First Amendment can serve as a limitation on the power of the grand jury to interfere with a witness' freedoms of association and expression").

In fact, the First Amendment's protection is often greater than that afforded by the Fourth Amendment alone. Indeed, even those cases applying a Fourth Amendment analysis give First Amendment interests independent weight, requiring "scrupulous exactitude" when expressive information is at stake. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)); *see Marcus v. Search Warrant*, 367 U.S. 717 (1961).

The Second Circuit has recognized that the Fourth Amendment does not serve as a substitute for First Amendment interests, because the rights are not coextensive. In *Tabbaa*, the court considered the border search of five U.S. citizens returning from a religious conference in Toronto. After concluding that the searches and detentions did not violate the Fourth Amendment, the Second Circuit conducted a separate First Amendment analysis, and declared that

> [o]ur conclusion that the searches constituted a significant or substantial burden on plaintiffs' First Amendment associational rights is unaltered by our holding that the searches were routine under the Fourth Amendment. As is clear from the above discussion, distinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.

509 F.3d at 102 n. 4.

In some cases, safeguards required by the Fourth Amendment may in practice satisfy the First Amendment as well. *See, e.g.*, *Zurcher*, 436 U.S. at 565; *United States v. Ramsey*, 431 U.S. 606, 623–24 (1977). But that does not mean the First Amendment lacks application to investigative activities. A criminal search warrant, carefully drawn and supported by probable cause, may overcome a countervailing First Amendment interest. But as the government's demands for information become more diffuse, implicating more and more protected information on a lower showing of relevance or need, the First Amendment calculus shifts too. *See Gibson*, 372 U.S. at 546; *Local 1814*, 667 F.2d at 269; *LaRouche*, 817 F.2d at 234–35; *Paton v. La Prade*, 469 F. Supp. 773 (D.N.J. 1978).

Here, as detailed in Mr. Moalin's Initial Memo of Law, at 8, the 2003 investigation of Mr. Moalin "did not find any connection to terrorist activity." It is inconceivable that the investigation did not also involve investigation of conduct and/or expression by Mr. Moalin fully protected by the First Amendment. *See*, *e.g.*, FBI San Diego Field Intelligence Group Assessment, dated June 15, 2011 (attached as Exhibit 1 to Mr. Moalin's Initial Memo of Law).

Yet it was that investigation that provided the link to Mr. Moalin years later, and led to the FISA-authorized electronic surveillance and search in 2007-08. In his pretrial motion challenging that FISA surveillance and search, Mr. Moalin explicitly referred to the limits on investigating a U.S. person's First Amendment activities. Here, the links in the investigative chain involved improper use and retention of protected First Amendment activity.

In addition, 18 U.S.C. §2339B(i) (which would apply directly to Count Two and indirectly to Counts One, Four, and Five) provides that, as a "Rule of construction," that "[n]othing in this section shall be construed or applied so as to abridge the exercise of rights guaranteed under the First Amendment to the Constitution of the United States." Here, the genesis of the investigation of Mr. Moalin was arguably (and should be assumed if the government continues to resist

disclosure that could resolve the issue) the result of improper interception/collection/retention of conduct and/or expression that was entirely protected by the First Amendment, and would therefore indisputably have "abridged" Mr. Moalin's First Amendment rights.

B. ***Mr. Moalin's Challenge to the Government's Interception/Surveillance of His Electronic Communications Pursuant to the Section 702 (50 U.S.C. §1881a)***

Regarding that portion of Mr. Moalin's Rule 33 motion addressing interception of Mr. Moalin's communications pursuant to Section 702 (50 U.S.C. §1881a), *see* Mr. Moalin's Initial Memo of Law, at 19-23, the government steadfastly resists any disclosure or admission, instead erecting the same stonewall it has presented in other cases around the country. *See United States v. Daoud*, 12 Cr. 723 (SJC) (N.D. Ill.) (Docket #63); *United States v. Qazi*, 12 Cr. 60298 (RNS) (S.D. Fla.) (Docket #131).

The government's uniform circling of the wagons, more than likely the result of decision-making at a level considerably above the prosecutors in this case, appears designed to protect NSA from disclosure of its illegal conduct and interference with its construction and operation of its vast electronic surveillance architecture that reaches into every U.S. (and international) home, business, and communication.

As a threshold matter, it is unclear to what extent the government, in its denial that Section 702 is relevant to this case or required notice to Mr. Moalin, relies on its policy of "parallel construction," discussed in the article by John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/15xWJwH (describing parallel construction as "just like money laundering – you work it backwards to make it clean"), that was cited in Mr. Moalin's Initial Memo of Law at 24, n.13. Any such sanitizing of an investigation's origins, or the basis for obtaining court authorization for electronic surveillance or searches (or anything else) cannot be

considered legitimate, or a substitute for complete and accurate disclosure.

In addition, due process mandates the disclosure of information in the government's possession if nondisclosure would "affect the outcome of [a] suppression hearing." *Smith v. Black*, 904 F.2d 950, 965 (5th Cir. 1990); *see also United States v. Gamez-Orduño*, 235 F.3d 453, 461 (9th Cir. 2000). Here, Mr. Moalin seeks suppression of evidence acquired via Section 702, a statute that does not operate on traditional probable cause or other *de novo* substantive review principles, further justifying disclosure. *See, e.g.*, *Michigan v. DeFillippo*, 443 U.S. 31, 39 (1979) (recognizing that statutes which, "by their own terms, authorize[] searches under circumstances which d[o] not satisfy the traditional warrant and probable-cause requirements of the Fourth Amendment," are on their face more constitutionally suspect).

Also, the government focuses exclusively on the telephone call referred to in the January 24, 2008, e-mail from FBI Special Agent Michael C. Kaiser to the government's Somali linguist, Liban Abdirahman, attached as Exhibit 6 to Mr. Moalin's Initial Memo of Law, a call that was not consummated. *See* Gov't Memo of Law, at 28.

That misses the point. The e-mail's reference to that interception – "We just heard from another agency that Ayrow tried to call Basaaly today, but the call didn't go through" – demonstrates that "another agency" (no doubt NSA, given subsequent public disclosures) *was potentially intercepting those communications on an ongoing basis*.

Moreover, to the extent the government knew – or did not know – Mr. Ayrow's telephone number, and was monitoring and/or intercepting it, that was extraordinarily relevant to the most important issues at trial. Indeed, the manner in which Mr. Ayrow was identified as the person trying to reach Mr. Moalin – voice exemplar (or recognition), human intelligence, or some other means – was just as essential to the critical contested issues at trial. If the government was mistaken in

its identification, that would make it only *more* relevant.

Also, SA Kaiser's January 24, 2008, e-mail establishes that the "other" interception was "used" against Mr. Moalin, as SA Kaiser issued investigative instructions to Mr. Abdirahman as a result. Nor does the single e-mail determine the limits of the interception(s), and the uses to which it was put against Moalin. There remain additional questions:

- were there prior Section 702 (or other) interceptions or monitoring that contributed in any way to the application for the initial FISA interception on Mr. Moalin's telephone (and which constituted the majority of the government's evidence at trial)?

- did the Section 702 (or other) interception or monitoring referred to in the January 24, 2008, e-mail contribute in any way to applications to extend the FISA surveillance beyond its initial term?

- did any Section 702 (or other) interception or monitoring occurring after the January 24, 2008, e-mail contribute in any way to applications to extend the FISA surveillance beyond its initial term?

- did any Section 702 (or other) interception or monitoring referred to in the January 24, 2008, e-mail, or occurring before or afterward, contribute in any way to applications to conduct a FISA-authorized search related to Mr. Moalin (which was ultimately executed)?

- did any Section 702 (or other) interception or monitoring referred to in the January 24, 2008, e-mail, or occurring before or afterward, contribute in any way to identification, collection, or development of any evidence in the case, or any information that led to evidence in the case, including questions asked of witnesses and/or instructions provided to investigators or others working for the government during the course of the investigation?

Also, the meaning of "derived" evidence has a long and developed pedigree in Fourth Amendment case law under the "fruit of the poisonous tree" doctrine. Evidence is "derived" from illegal surveillance when it is the "product" of that surveillance or "is otherwise acquired as an indirect result of the unlawful search, up to the point at which the connection with the unlawful search becomes 'so attenuated as to dissipate the taint.'" *Murray v. United States*, 487 U.S. 533, 536-37 (1988) (quoting *Nardone v. United States*, 308 U.S. 338, 341(1939)).

Thus, "derived" evidence is a "well established term of art" in the search context, carrying a meaning that pre-dates and was incorporated into FISA. *Chandler v. U.S. Army*, 125 F.3d 1296, 1304 (9th Cir. 1997); *see United States v. Giordano*, 416 U.S. 505, 531-32 (1974) (interpreting the meaning of derived evidence in relation to a sequence of electronic intercepts and wiretap orders); S. Rep. No. 95-701, at 13 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3982 ("[FISA] embodies a legislative judgment that court orders and other procedural safeguards are necessary to ensure that electronic surveillance by the U.S. government within this country conforms to the fundamental principles of the Fourth Amendment").

In that framework, both the Fourth Amendment and the statute attach significant weight and meaning to "derived" evidence. In fact, a robust definition of "derived" evidence is essential to the FISA Amendments Act's notice provision and FISA's overall statutory scheme. The notice requirement in §1806(c) has a specific

procedural purpose: it is closely tied to the suppression provisions that immediately follow in §§1806(e) and 1806(g). In those sections Congress provided that aggrieved persons must be afforded an adequate opportunity to challenge and suppress evidence obtained or derived from electronic surveillance.

As the statutory scheme makes plain, these suppression provisions depend on notice – they lack vitality and impact unless a defendant is first given notice of the basis for the government's search. *Cf. United States v. Eastman*, 465 F.2d 1057, 1062–63 & n. 13 (3d Cir. 1972) (Title III's statutory notice provision was "intended to provide the defendant whose telephone has been subject to wiretap an opportunity to test the validity of the wiretapping authorization").

In addition, the "use" of Section 702 interceptions or monitoring in the criminal investigation of Mr. Moalin is not the only manner in which its application to Mr. Moalin's electronic communications might be unlawful in this case. Indeed, in that same January 24, 2008, e-mail SA Kaiser advises Mr. Abdirahman that "We're extremely interested in getting real-time info (location/new #s) on Ayrow." Exhibit 6 to Mr. Moalin's Initial Memo of Law .

Given that the U.S. government had previously attempted to target Mr. Ayrow via missile attack (unsuccessfully),[5] and ultimately did so successfully May 1, 2008, and that journalists with access to information and documents disclosed by former NSA contractor Edward Snowden have already publicly announced they are working on articles regarding how the NSA's surveillance programs have been used as part of the U.S.'s targeted assassinations programs, the implications of "real time" information on Mr. Ayrow's whereabouts in early 2008 are obvious, if not altogether

---

[5] Michael R. Gordon & Mark Mazzetti, "U.S. Used Base in Ethiopia to Hunt Al Qaeda," *The New York Times*, February 23, 2007, available at http://www.nytimes.com/2007/02/23/world/africa/23somalia.html?pagewanted=all ("On Jan. 7, one day after the AC-130s arrived in Ethiopia, the airstrike was carried out near Ras Kamboni, an isolated fishing village on the Kenyan border. According to American officials, the primary target of the strike was Aden Hashi Ayro")

ominous. *See* Jenny Barchfield, "Glenn Greenwald, Jeremy Scahill Working on New NSA Revelations," *Associated Press*, September 28, 2013, available at <http://www.huffingtonpost.com/2013/09/29/glenn-greenwald-jeremy-scahill-nsa-assassination_n_4010405.html>.

Such use of Section 702 authority would be beyond the scope of anything authorized by Congress or approved by the FISC – unless, of course, that is the subject of another set of secret procedures and protocols yet to be exposed and subsequently acknowledged. In any event, it would be unlawful, unconstitutional, and subject to sanction via suppression.

Moreover, the government's claim that Section 702 is not relevant to this case, and/or that notice is not required, is belied by the substantial redactions within that section of the government's Memo of Law. Otherwise, a curt, categorical "no" would have been the appropriate response.

Accordingly, Mr. Moalin's motion for discovery, a hearing, and, ultimately, suppression and a new trial, should be granted.

C. *The Court Should Order Disclosure to Cleared Defense Counsel the FISA Applications and/or the CIPA §4 Motions*

The government's continued concealment via heavy redactions – why a section discussing exculpatory material would require redaction begs the question entirely (*see* Gov't Memo of Law, at 27-29) – and *ex parte* submissions (*see* Docket #354) merely reinforce the need for adversary proceedings that are meaningful, and which afford Mr. Moalin a fair chance in this motion.

The cost of secret proceedings and submissions is not abstract in this context. As the few publicly published opinions of the FISC make clear, NSA has routinely lied to the FISC, and even, in functional terms, to itself.

Mr. Moalin's Initial Memo of Law, at 27-28, discussed the FISC's 2011 Opinion's catalogue of NSA's misstatements to the FISC and NSA's inability to implement its programs within the confines of Congressional authorization and/or FISC approval – even to the extent of NSA's inability even to discern the difference

or quantify its level of non-compliance. *Id*. *See also* Exhibit 9 to Mr. Moalin's Initial Memo of Law.

That 2011 FISC opinion referred to a 2009 FISC Opinion that was released to the public after this motion was filed. That opinion, by FISC Judge Reggie B. Walton (who also sits as a District Judge in the District for the District of Columbia) provides further and compelling proof that NSA persistently lies to, conceals from, and misleads (affirmatively and by silence) the FISC, that NSA cannot be trusted even to train its own employees adequately, or even be able to determine for itself the limits on its surveillance activities consistent with statute or FISC Orders. *See In re Production of Tangible Things From [***Redacted***]*, Docket No. BR 08-13 (FISC March 2, 2009) (a copy of which is attached hereto as Exhibit 1).

Judge Walton's FISC opinion demonstrates the plethora of statutory violations that pervade the NSA's electronic surveillance programs, including those at issue herein.[6] For example, Judge Walton's March 2009 FISC opinion includes the following passages:

- "[t]he government's submission suggests that its non-compliance with the Court's orders resulted from a belief by some personnel within the NSA that some of the Court's restrictions on access to the BR [Business Records] metadata applied only to "archived data" . . . That interpretation strains credulity. . . such an illogical interpretation of the Court's Orders renders compliance

[6] While the government, at 18 of its Memo of Law, contends that Section 215 lacks a suppression mechanism, surely the Court's supervisory power provides ample authority to sanction the government for a series of lies and violations that otherwise would continue without adverse consequence to anyone but Mr. Moalin. However, the Court need not decide that issue because the concurrent multiple Constitutional violations provide sufficient remedial vehicles for Mr. Moalin.

with the RAS [Reasonable, Articulable Suspicion] requirement merely optional." *Id*., at 5;

- "[t]he government compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC." *Id*., at 6;

- "[r]egardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations fo the minimization procedures set forth in FISC orders and designed to protect [**REDACTED**] call detail records pertaining to telephone communications of US persons located within the United States who are not the subject of any FBI investigation and whose call detail information could not otherwise have been legally captured in bulk." *Id*., at 8-9;

- "[i]n summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This 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. *The minimization procedures*

proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systematically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively." *Id*., at 10-11 (emphasis added);

- "[t]he record before the Court strongly suggests that, from the inception of this FISA BR program, the NSA's data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures." *Id*., at 14-15; and

- "[u]nder these circumstances, *no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures*. In fact, the government acknowledges that, *as of August 2006, "there was no single person who had a complete understanding of the BR FISA system architecture*." *Id*., at 15 (emphasis added). *See also* Scott Shane, "Court Upbraided N.S.A. on Its Use of Call-Log Data," *The New York Times*, September 10, 2013, available at <http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html?pagewanted=all&_r=0> (noting that, according to a senior U.S. intelligence official who briefed reporters just prior to release of the 2009FISC opinion, "only about 10 percent of 17,800 phone numbers on the alert list in 2009 had met [the RAS] test," and that "'[t]here was nobody at N.S.A. who really had a full understanding of how the program was operating at the time").

Judge Walton also recognized the FISC's limitations as a watchdog, pointing out that "in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of US persons as required by applicable minimization procedures." *Id.*, at 12.

Elaborating, Judge Walton noted that "[t]o approve such a program, the Court must have every confidence that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders." *Id.* Yet, he concluded, "[t]he Court no longer has such confidence." *Id.*

Judge Walton's lack of confidence was well-founded, and validated by NSA's continued non-compliance. As if Judge Walton's 2009 FISC opinion were insufficient to demonstrate NSA's abject inability – whether deliberate or simply through inexcusably irresponsible negligence or cavalier incompetence – to comply, a subsequent August 13, 2009, report the government submitted to the FISC revealed even more non-compliance issues beyond the myriad enumerated in Judge Walton's opinion, and which were discovered after issuance of that Opinion. *See* Report of the United States, *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Docket No. BR 09-09, August 13, 2009, (hereinafter "US Report, Docket BR 09-09"), attached hereto as Exhibit 2.[7]

Further violations of the FISC's Orders included, for example, (a) permitting employees of other government agencies to have external and

[7] NSA's continued non-compliance, even through 2011 as described in Judge Bates's FISC opinion (*see* Exhibit 9 to Mr. Moalin's Initial Memo of Law), establishes that the FISC's complaints, and even its attempts at remedial measures, are ineffectual as long as the process remains secret. That is the inevitable result of secrecy, which is why the adversary process has evolved as the best guarantor of a fair adjudicative process.

unsupervised access to the NSA database; (b) failing to audit for compliance issues – at any point over the lifespan of the program – a database used to store information retrieved from the NSA databases; and (c) use of software with a feature permitting analysts to pull more information than NSA was authorized to retrieve. *Id.*[8]

Thus, continued secrecy will invariably lead to continued abuse and violations, and to accommodate the government's request that cleared defense counsel be denied access will serve simply to perpetuate that outcome. The public record – and who knows (certainly not defense counsel) what still remains classified – compels but one conclusion: NSA cannot be trusted, despite repeated chances, and one of the principal reasons is the absence of any accountability. Adversary proceedings, even pursuant to the Classified Information Procedures Act, provide some measure of accountability – at least in the context of *this case*, which is the appropriately narrow context that applies – and Mr. Moalin will surely suffer if "business as usual" in this regard – denying cleared defense counsel access – ensues.

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 a new trial, and/or compel the discovery demanded in this motion, and/or conduct the evidentiary hearings requested herein.

Dated: 10 October 2013
New York, New York

Respectfully submitted,

S/ Joshua L. Dratel
JOSHUA L. DRATEL

[8] Thus, even if "trust, but verify" were the standard – not justifiable in this instance, given NSA's unbroken record of violation and recidivism, and the lack of any means of effective general or specific deterrence – that would still require meaningful third-party verification, *i.e.*, genuine adversary access and participation by cleared defense counsel.

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
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