

1 monetary instruments in violation of 18 U.S.C. §1956(h); (4) providing material
2 support to terrorists in violation of 18 U.S.C. §2339A(a); and (5) providing material
3 support to a foreign terrorist organization in violation of 18 U.S.C. §§2339B(a)(1) and
4 (2). (Ct. Dkt. 147). Counts One, Two and Three were charged against all Defendants,
5 Count Four against Moalin alone, and Count Five against all Defendants except Nasir.

6 **The FISA Motion**

7 On December 9, 2011, Defendants, among other things, moved to suppress
8 wiretap evidence obtained pursuant to a Foreign Intelligence Surveillance Act
9 (“FISA”) warrant, evidence seized pursuant to a search warrant of Defendant Moalin’s
10 home; and statements made at the time of Defendant Moalin’s arrest. (Ct. Dkt. 92).
11 On October 17, 2012, the court issued an order denying the motion to suppress
12 evidence seized from Moalin’s residence, denied the motion to suppress statements,
13 and continued the FISA wiretap motion.

14 Defendants’ FISA motion challenged the Government’s use of electronic
15 surveillance obtained pursuant to 50 U.S.C. §1806 (Title I of FISA) and those
16 collections obtained after the enactment of Section 702 (50 U.S.C. §1881a) of the FISA
17 Amendments Act of 2008 (“FAA”). On June 4, 2012, in an order placed under seal
18 with the Court Security Officer (“FISA Order”), the court denied Defendants’ motion
19 to suppress FISA intercepts and provided the parties notice of that fact. (Ct. Dkt. 146).

20 On March 9, 2012, in reply to the Government’s opposition to the motion to
21 dismiss FISA materials, Defendants repeated their request that defense counsel
22 possessing appropriate security clearances be granted access to the FISA warrant
23 applications and pertinent orders of the Foreign Intelligence Surveillance Court
24 (“FISC”). Among other things, Defendants argued that the electronic surveillance was
25 obtained in violation of FISA, the First and Fourth Amendments, and Brady v.
26 Maryland, 373 U.S. 83 (963). Defendants also argued that the minimization protocols
27 were defective. (Ct. Dkt. 131).

28

1 The CIPA Motions

2 On March 9, 2012, Defendants jointly and preemptively moved to deny the
3 Government's anticipated request for an ex parte and in camera review pursuant to
4 Section 4 of the Classified Information Protection Act ("CIPA"), 18 U.S.C. App. 3 §4.

5 On March 23, 2012, the Government filed a response to Defendants joint motion to (1)
6 deny the ex parte CIPA filing and (2) compel disclosure of the CIPA materials to
7 cleared defense counsel. To assist the court in its review of CIPA-related materials for
8 purposes of Brady, the First and Fourth Amendments, Fed.R.Crim.P. 16, and the Jencks
9 Act, the court requested, and Defendants jointly submitted under seal, a memorandum
10 identifying seven broad defense theories as well as specific evidence sought to be
11 discovered in the Government's CIPA submission. (Ct. Dkt 133-35).

12 Ultimately, the Government submitted five requests for a protective order under
13 CIPA. On August 28, 2012, the court completed its CIPA review of the materials
14 provided by the Government and dated March 21, 2012, June 1, 2012, and August 22,
15 2012.¹ On August 28, 2012, the court filed its first CIPA order under seal with the
16 Court Security Officer and provided notice to all parties of its entry. The court also
17 ordered the Government to provide to Defendants two substituted statements as
18 permitted by CIPA. (Ct. Dkt. 183). On January 17, 2013, the court granted the motion
19 for a protective order concerning two additional submissions by the Government and
20 dated January 2, 2013, and January 17, 2013. (Ct. Dkt. 253).

21 On January 28, 2013, Defendants filed under seal a motion for Court Ordered
22 Remedies to Address the Government's Violation of Brady. (Ct. Dkt 271). On January
23 30, 2013, the court issued an order addressing several discovery-related issues raised
24 in Defendants' motion and requesting that the Government submit for in camera review
25 the redacted emails at issue. (Ct. Dkt. 273). Ultimately, the court concluded that the
26 unredacted emails need not be produced pursuant to Brady, Fed.R.Crim.P. 16, or the

27
28 ¹ Upon completion of its initial review of the submitted CIPA materials, the court requested in a sealed order that the Government submit additional classified documents for in camera review.

1 Jencks Act. (Ct. Dkt. 279).

2 **The Rule 15 Depositions**

3 On July 20, 2012, Defendants filed a second motion to take the depositions of
4 eight prospective defense witnesses in Somalia. (Ct. Dkt. 154). Defendants
5 represented that these individuals received money transfers from Defendant Moalin and
6 possessed direct knowledge of how the transferred money was spent. (Ct. Dkt. 154 at
7 p.2:13-14). The court denied the motion without prejudice and referred the parties to
8 Magistrate Judge William V. Gallo to discuss the Rule 15 depositions. On September
9 6, 2012, after consulting with the parties, Magistrate Judge Gallo ordered the eight
10 depositions to proceed in Djibouti, Djibouti, (Ct. Dkt. 189), and set forth the logistics
11 for the witness depositions. (Ct. Dkt. 195). The depositions (except the deposition of
12 Farah Shidane) went forward in Djibouti from November 11-15, 2012. The videotaped
13 depositions were viewed by the jury during Defendants' case-in-chief.

14 **The Trial**

15 The jury trial commenced on January 28, 2013. The Government presented 13
16 witnesses over five days and the Defense presented 11 witnesses over five days,
17 including eight video-taped depositions taken pursuant to Fed.R.Crim.P. 15(a). On
18 February 22, 2013, after 17 days of trial and deliberations, the jury returned guilty
19 verdicts on all counts alleged in the second superseding indictment.²

20 **Recent Public Disclosures**

21 On June 8, 2013, The Washington Post reported on disclosures made by Edward
22 Snowden, a former NSA contract employee. As described by Defendants, “[t]he
23 documents Mr. Snowden provided revealed the existence of the scope of NSA’s
24 electronic surveillance, interception, and collection, including communications data
25 relevant to U.S. persons.” (Motion at p.7:12-14). In broad brush, the disclosures
26 revealed the existence of several classified United States surveillance programs and

27
28 ² On September 21, 2012, the court appointed Magistrate Judge Gallo as a special master to oversee the depositions and authorized the Magistrate Judge to exercise those duties specifically enumerated in Fed.R.Civ.P. 53(c).

1 their scope. As reported by the Associated Press, on September 26, 2013, NSA director
2 Keith B. Alexander confirmed that one goal of the NSA is to collect and store all phone
3 records of American citizens. Senators: Limit NSA Snooping into US Phone Records,
4 Associated Press, October 15, 2013.

5 In addition to the so-called Snowden disclosures, Defendants also cite several
6 statements made by Sean Joyce, Deputy Director of the FBI, before the House
7 Permanent Select Committee on Intelligence to support their Rule 33 motion.
8 Defendants highlight that Deputy Director Joyce stated that material obtained from the
9 NSA program resulted in the investigation of terrorist activities, including the present
10 case. (Def't Exh. 2). Deputy Director Joyce also stated that the NSA provided a
11 telephone number in San Diego "that had indirect contact with an extremist outside the
12 United States." Using this telephone number the FBI "served legal process to identify
13 the subscriber to this telephone number." He further stated, "However, the NSA using
14 the business record FISA [Section 215] tipped us off that this individual had indirect
15 contacts with a known terrorist overseas." Based largely upon this investigation, the
16 FBI applied to the FISC for FISA warrants and "disrupt[ed] this terrorist activity." Id.

17 On July 18, 2013, at a conference at the Aspen Security Forum in Aspen
18 Colorado, General Alexander reportedly repeated that, based on information obtained
19 in Somalia, a telephone number was traced to San Diego. The telephone number was
20 traced to Defendant Moalin and an investigation was commenced against him "in 2003
21 but didn't have enough information to go up on." (Def't Exh. 3).

22 On July 31, 2013, Deputy Director Joyce provided testimony before the Senate
23 Judiciary Committee. He reportedly stated that an FBI investigation of Defendant
24 Moalin was opened "in 2003 based on a tip. We investigated that tip. We found no
25 nexus to terrorism and closed the case." (Def't Exh. 5). He also stated that, in 2007,
26 the NSA advised the FBI that the San Diego telephone number was in contact with
27
28

1 members of al-Shabaab.³ Acting on this information, the FBI “served legal process to
2 identify the unidentified phone number. We identified [Defendant Moalin].” Id.

3 **Classified Facts Summary**

4 The court incorporates the classified factual summary set forth in the
5 Government’s opposition filed under seal.

6 **DISCUSSION**

7 **Legal Standards**

8 The court notes that neither Defendants nor the Government sets forth the legal
9 standard governing this motion. Under Rule 33(a), the court has broad authority to
10 grant a motion for new trial whenever “the interest of justice so requires.”
11 Fed.R.Crim.P. 33(a); United States v. Young, 17 F.3d 1201, 1205 (9th Cir. 1994).
12 Notably, Defendants raise no typical arguments for a new trial: sufficiency of the
13 evidence, evidentiary rulings, instructional challenge, or prosecutorial misconduct.
14 Rather, Defendants focus on two sealed orders of the court: the order denying the
15 motion to suppress FISA intercepts and the order granting the Government’s motion
16 for a protective order under CIPA.

17 Defendants broadly argue that recent revelations by Snowden and Government
18 officials regarding NSA surveillance in this particular case warrant the suppression of
19 all intercepted conversations. Although the present motion does not neatly fit into the
20 category of newly discovered evidence, it is nonetheless helpful to set forth the
21 standard for such a claim. The court considers the following five part test to determine
22 whether to grant a new trial based on newly discovered evidence: (1) the evidence must
23 be newly discovered; (2) the failure to discover the evidence sooner must not be the
24 result of a lack of diligence on the defendant’s part; (3) the evidence must be material

25
26 ³ Al-Shabaab, a violent and brutal militia group, was designated by the U.S.
27 Department of State as a Foreign Terrorist Organization on February 26, 2008. (Ct.
28 Dkt. 147 ¶1). “Throughout al-Shabaab’s war against the TFG (Somalia’s Transitional
Federal Government) and its Ethiopian and African Union supporters, al-Shabaab used
harassment and targeted assassinations of civilians, improvised explosive devices,
mines, mortars, automatic weapons, suicide bombings, and general tactics of
intimidation and violence.” (Id. ¶2).

1 to the issues at trial; (4) the evidence must be neither cumulative nor merely
2 impeaching; and (5) the evidence must indicate that a new trial would probably result
3 in acquittal. United States v. Sarno, 73 F.3d 1470, 1507 (9th Cir. 1995).

4 Setting aside the issue of admissibility of the public revelations of the NSA
5 program of securing telephone metadata, the public disclosure of the NSA program
6 adds no new facts to alter the court's FISA and CIPA rulings. Because the court has
7 already considered and addressed many of the FISA and CIPA arguments from a
8 federal and constitutional law perspective, the present motion is akin to a motion for
9 reconsideration. Under the reconsideration standard, the court is authorized to alter its
10 prior rulings based upon newly discovered evidence, intervening change of law, or
11 clear error. See School Dist. N. 1J, Multnomah Cty. v. ACandS, Inc., 5 F.3d 1255,
12 1262 (9th Cir. 1993). The court notes that the newly discovered evidence prong is not
13 particularly useful in this case to the extent the NSA revelations are newly discovered
14 by Defendants. The mere existence of the NSA program has no evidentiary value in
15 and of itself, and the telephony metadata collected from the NSA program was either
16 provided to the defense by means of the intercepted telephone calls produced in
17 discovery or considered by this court under its FISA and CIPA responsibilities.
18 Similarly, the intervening change of law prong is not useful to the Defendants because
19 they cite no intervening change of law. To the extent the clear error prong applies, the
20 court notes that the clear error standard is analogous to the "interests of justice"
21 requirement of Rule 33.

22 **The Motion**

23 Defendants raise three main arguments in support of their motion for new trial:
24 (1) The NSA intercepts and/or collection of electronic data related to Defendant Moalin
25 violated the First and Fourth Amendments and FISA; (2) cleared defense counsel
26 should have previously been, and, should now be provided with the Government's
27 under seal response to their FISA motion, including the FISA applications and
28 warrants, and the ex parte request for a protective order under CIPA; and (3) the

1 Government failed to provide necessary Rule 16 discovery and exculpatory materials
2 under Brady. To the extent possible, each argument is discussed in this publicly
3 available order.⁴

4 The NSA Surveillance

5 Defendants argue that the collection of telephony metadata violated Defendant
6 Moalin's First and Fourth Amendment rights. At issue are two distinct uses of
7 telephone metadata obtained from Section 215. The first use involves telephony
8 metadata retrieved from communications between third parties, that is, telephone calls
9 not involving Defendants. Clearly, Defendants have no reasonable expectation of
10 privacy to challenge any use of telephony metadata for calls between third parties. See
11 Steagald v. United States, 451 U.S. 204, 219 (1981) (Fourth Amendment rights are
12 personal in nature); Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) ("Fourth
13 Amendment rights are personal rights which, like some other constitutional rights, may
14 not be vicariously asserted."); United States v. Verdugo-Urquidez, 494 U.S. 259, 265
15 (1990) (the term "people" described in the Fourth Amendment are persons who are part
16 of the national community or may be considered as such). As noted in Steagald, "the
17 rights [] conferred by the Fourth Amendment are personal in nature, and cannot bestow
18 vicarious protection on those who do not have a reasonable expectation of privacy in
19 the place to be searched." 451 U.S. at 219. As individuals other than Defendants were
20 parties to the telephony metadata, Defendants cannot vicariously assert Fourth
21 Amendment rights on behalf of these individuals. To this extent, the court denies the
22 motion for new trial.

23 The second use of telephony metadata involves communications between
24 individuals in Somalia (or other countries) and Defendant Moalin. The following
25 discusses whether Defendant Moalin, and other Defendants through him, have any
26 reasonable expectation of privacy in telephony metadata between Moalin and third

27
28 ⁴ The court informs the parties that this is the only order addressing the issues
raised in the Rule 33 motion. No order has been filed under seal to address
Defendants' arguments.

1 parties, including co-defendants.

2 **The Fourth Amendment**

3 Defendants contend that they have a Fourth Amendment reasonable expectation
4 of privacy in the collection of telephony metadata for communications between third
5 parties and Defendants.⁵ In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme
6 Court addressed whether the Fourth Amendment was violated when the telephone
7 company, at police request and without a warrant, installed a pen register to record
8 numbers dialed from petitioner Smith's home. Based upon information received from
9 the victim, the police believed that Smith was involved in a robbery. After the robbery,
10 the victim received threatening and obscene telephone calls from an individual
11 identifying himself as the robber. Id. at 737. The device installed recorded the
12 telephone numbers dialed from the defendant's home but did not record the contents
13 of the conversation. When the victim received another telephone call from Smith, the
14 police obtained a search warrant to search Smith's home.

15 Consistent with Katz v. United States, 389 U.S. 347 (1967), the Supreme Court
16 held that the application of the Fourth Amendment "depends on whether the person
17 invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate
18 expectation of privacy' that has been invaded by government action." Smith, 442 U.S.
19 at 740. A justifiable, reasonable, or legitimate expectation of privacy is one where (1)
20 the defendant, by his conduct, has "exhibited an actual (subjective) expectation of
21 privacy," and (2) the individual's subjective expectation of privacy is "one that society
22 is prepared to recognize as 'reasonable,'" that is, whether the individual's expectation,
23 "viewed objectively is 'justifiable under the circumstances.'" Id. (quoting Katz, 389
24 U.S. at 351-62).

25 The Supreme Court noted that someone who uses a telephone has "'voluntarily
26 conveyed numerical information to the telephone company and exposed' that

28 ⁵ The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

1 information to its equipment in the ordinary course of business,” and therefore has
2 “assumed the risk that the company would reveal to police the numbers he dialed.” Id.
3 at 744. The Supreme Court has consistently held “that a person has no legitimate
4 expectation of privacy in information he voluntarily turns over to third parties.” Id.;
5 United States v. Miller, 425 U.S. 435 (1976) (“the Fourth Amendment does not prohibit
6 the obtaining of information revealed to a third party and conveyed by him to United
7 States authorities, even if the information is revealed on the assumption that it will be
8 used only for a limited purpose and the confidence placed in the third party will not be
9 betrayed”).

10 In United States v. Reed, 575 F.3d 900 (9th Cir. 2009), the Government, acting
11 without a warrant, requested that the telephone company install a pen register and trap
12 and trace device on the defendant’s telephone. The pen register and trap and trace
13 device provided “call data content,” that is, data about “call origination, length, and
14 time.” Id. at 914. The defendants argued that the call data content had to be
15 suppressed under the Fourth Amendment. Citing Smith, the Ninth Circuit determined
16 that defendants had no Fourth Amendment “expectation of privacy” in the data and
17 affirmed the district court’s denial of the motion to suppress. Id. Further, the Ninth
18 Circuit has repeatedly held that an individual does not have a reasonable expectation
19 of privacy in business records such as power company consumption records, telephone
20 records, bank records, or motel registration records. United States v. Golden Valley
21 Elec. Ass’n, 689 F.3d 1108, 1116 (9th Cir. 2012); United States v. Miller, 425 U.S.
22 436, 440 (1976) (“the Fourth Amendment does not prohibit the obtaining of
23 information revealed to a third party and conveyed by him to the United States
24 authorities”); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993) (holding it
25 was “evident” that the defendant did not have any justifiable privacy interest in
26 telephone records obtained from the service provider); United States v. Qing Li, 2008
27 WL 789899 *4 (S.D. Cal. Mar. 20, 2008, No. 07cr2915 JM) (defendant lacks a
28 reasonable expectation of privacy in Internet Protocol log-in histories and addressing

1 information).

2 In light of these persuasive and binding authorities, Defendants argue that the
3 court should blaze a new path and adopt the approach to the concept of privacy set
4 forth by Justice Sotomayor in her concurrence in United States v. Jones, __U.S.__, 132
5 S.Ct. 945, 954-964 (2012). In Jones, the Supreme Court considered whether the
6 installation and subsequent monitoring of a Global Positioning System tracking device
7 on an automobile by the police without a valid warrant and without the individual's
8 consent violated the Fourth Amendment. Noting that Fourth Amendment
9 jurisprudence, up to the latter half of the 20th century, was tied to common-law trespass
10 principles, the majority held that "[w]here, as here, the Government obtains information
11 by physically intruding on a constitutionally protected area," the Fourth Amendment
12 is violated. Id. at 950 n.3, 954. As noted by Defendants, Justice Sotomayor stated that
13 the recent rise of the digital era of cell phones, internet, and email communications may
14 ultimately require a reevaluation of "expectation of privacy in information voluntarily
15 disclosed to third parties." Id. at 957. Defendants extrapolate from this dicta that the
16 court should recognize that Defendant Moalin had a reasonable expectation of privacy
17 cognizable under the Fourth Amendment that the Government would not collect either
18 individual or aggregated metadata.

19 The difficulty with Defendants' argument is twofold. First, the use of pen
20 register-like devices - going back to Samuel Morses's 1840 telegraph patent - predates
21 the digital era and cannot be considered a product of the digital revolution like the
22 internet or cell phones. See Samuel F.G. Morse, Improvement in the Mode of
23 Communicating Information by Signals by the Application of Electro-Magnetism, U.S.
24 Patent 1647, June 20, 1840, page 4 column 2. In short, pen register-like devices
25 predate the internet era by about 150 years and are not a product of the so-called digital
26 revolution - the basis for the concerns articulated by Justice Sotomayor. Second, and
27 more importantly, the Supreme Court specifically and unequivocally held in Smith that
28 retrieval of data from a pen register by the Government without a search warrant is not

1 a search for Fourth Amendment purposes. 442 U.S. at 744. Because individuals
2 voluntarily convey numerical information to the telephone company to complete a
3 telephone call, one cannot possess a reasonable expectation of privacy in the telephone
4 number dialed (as opposed to the content of the conversation). Id. For these reasons,
5 the court declines Defendants’ invitation to depart from well-established precedent.

6 Here, when Defendant Moalin used his telephone to communicate with third
7 parties, whether in Somalia or the United States, he had no legitimate expectation of
8 privacy in the telephone numbers dialed. The calls were routed through the
9 communications company and its switching equipment in the ordinary course of
10 business. While Defendant Moalin may have had some degree of a subjective
11 expectation of privacy, that expectation is not “one that society is prepared to recognize
12 as reasonable.” Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (quoting Katz, 389 U.S.
13 at 361). Furthermore, where the calls were initiated by third parties, whether from
14 Somalia or other countries, Defendant Moalin’s subjective expectation of privacy is
15 even further diminished because Defendant Moalin cannot assert Fourth Amendment
16 principles on behalf of third parties. The court could not locate any authorities, nor do
17 Defendants cite any pertinent authorities, that recognize any expectation of privacy in
18 the receipt of telephone call data from a third party in a foreign country. As in Smith,
19 because the metadata was obtained through communications companies and their
20 switching equipment, Defendant Moalin “cannot claim that his property was invaded
21 or that police intruded into a ‘constitutionally protected area.’” 442 U.S. at 741.⁶
22 While technology continues to advance through the implementation of new devices and
23 methods, the legal analysis remains fairly constant: whether “the government violate[d]
24 a subjective expectation of privacy that society recognizes as reasonable.” Kyllo v.
25 United States, 533 U.S. 27, 33 (2001). For the above stated reasons, Defendant’s

26
27 ⁶ As set forth above, Defendant Moalin lacks standing to challenge the metadata
28 collected in reference to communications initiated by third parties. The Fourth
Amendment rights are “personal in nature” and Defendant Moalin cannot assert any
Fourth Amendment right on behalf of any party subject to the collection of telephone
metadata. See Steagald, 451 U.S. 204, 219.

1 minimal subjective belief in the privacy of telephony metadata is not one that society
2 has adopted.

3 The FISC has similarly determined that individuals like Defendant Moalin
4 cannot successfully assert a cognizable Fourth Amendment claim to telephony
5 metadata. In In re Application of the Federal Bureau of Investigation for an Order
6 Requiring the Production of Tangible Things, 2013 WL 5307991, *3 (For. Intell. Sur.
7 Ct. Aug. 29, 2013), the court found that a Section 215 order for telephony metadata
8 does not implicate the Fourth Amendment.

9 [B]ecause the Application at issue here concerns only the production of
10 call detail records or ‘telephony metadata’ belong to a telephone company,
11 and not the contents of communications, Smith v. Maryland compels the
12 conclusion that there is no Fourth Amendment impediment to the
collection [T]his court finds that the volume of records being
acquired does not alter this conclusion. Indeed, there is no legal basis for
the Court to find otherwise.

13 Defendants also vigorously contend that “the long-term recording and
14 aggregation of telephony metadata constitutes” an impermissible Fourth Amendment
15 search. (Reply at p. 6:7-8). The court notes that the preservation of “long-term
16 recordings” of telephony metadata played a minor role in the underlying
17 investigations.⁷ At the time of oral argument, defense counsel argued that Jewel v.
18 National Sec. Agency, 673 F.3d 902 (9th Cir. 2011) supports their position. There, the
19 plaintiff filed a putative class action on behalf of all Americans who were subscribers
20 of AT&T. Plaintiff alleged that the Government attached surveillance devices to
21 AT&T’s network. Id. at 906. The district court dismissed the action on standing
22 grounds. The central, merits-based allegation in Jewel arose “from claims that the
23 federal government, with the assistance of major telecommunications companies,
24 engaged in widespread warrantless eavesdropping in the United States following the
25 September 11, 2001, attacks.” Id. at 905. Shortly after the 911 attacks, President Bush

26
27 ⁷ The court declines to reach Defendants’ generalized arguments that (1) the
28 NSA involvement in surveillance activities was overbroad or (2) the NSA violated
orders by the FISC. Such public revelations and the ensuing debates in public and
political arenas do not alter or lessen this court’s responsibility to apply constitutional
and other relevant legal principles to this motion.

1 authorized “a terrorist surveillance program to detect and intercept al Qaeda
2 communications involving someone here in the United States.” Id. at 912. Plaintiff
3 alleged that the Government acquired the content of all email, internet, and telephone
4 communications. The court concludes that Jewel is not helpful to Defendants. First,
5 the merits involved the alleged eavesdropping on the content of the communications,
6 not just the telephony metadata. Second, the issues addressed in Jewel related to
7 standing, and not the Fourth Amendment. Id. at 905 (the issue is whether the plaintiff
8 had “standing to bring their statutory and constitutional claims”).

9 In sum, the court denies the motion for new trial based upon the alleged violation
10 of the Fourth Amendment.

11 **The First Amendment**

12 Defendants raise a generalized First Amendment challenge. In broad brush,
13 Defendants argue that “the 2003 investigation of Mr. Moalin ‘did not find any
14 connection to terrorist activity.’ It is inconceivable that the investigation did not also
15 involve investigation of conduct and/or expression by Mr. Moalin fully protected by
16 the First Amendment.” (Reply at p.15:12-14). Defendants cite no evidence nor
17 provide legal authority to support the proposition that Defendant Moalin’s First
18 Amendment rights were violated in any manner.

19 In sum, the court denies the motion for new trial based upon the alleged violation
20 of the First Amendment.

21 The FISA and CIPA Section 4 Arguments

22 Defendants argue that the Government did not comply with the provisions of
23 FISA and CIPA. The FISA and CIPA challenges are not addressed herein but in the
24 court’s previous sealed orders. With respect to the FISA and CIPA challenges, the
25 court notes that the arguments do not identify any newly discovered evidence,
26 intervening change in law, or clear error warranting reconsideration of its FISA and
27 CIPA orders.

28 In sum, the court denies the motion for new trial based upon the alleged violation

1 of FISA and CIPA.

2 Renewed Motion to Gain Access to FISA and CIPA Materials

3 In a well-presented argument, Defendants contend that cleared defense counsel
4 should have been earlier and should now be provided with all CIPA and FISA-related
5 materials (including FISA applications, exhibits, and FISC orders). Legal authorities
6 that have addressed this precise issue have uniformly rejected this argument. While
7 counsel may have security clearances, classified information may be disclosed only to
8 individuals who both possess the requisite clearance and additionally have a need to
9 know the information at issue. See Executive Order 13526, §§4.1(a) and 6.1(dd);
10 United States v. Sedaghaty, 728 F.3d 885, 908-09 (9th Cir. 2013); United States v.
11 Mejia, 448 F.3d 436, 458 (D.C. Cir 2006); Baldrawi v. Dept. of Homeland Security,
12 596 F. Supp. 2d 389, 400 (D. Conn. 2009) (counsel without need to know properly
13 denied access to classified information despite holding a security clearance): United
14 States v. Libby, 429 F. Supp. 2d 18, (D. D.C.), amended, 429 F. Supp. 2d 46 (D. D.C.
15 2006) (security clearance alone does not justify disclosure because access to classified
16 information is permitted only upon a showing that there is a “need to know”).

17 Here, the court reviewed all materials submitted under seal and concluded that
18 such ex parte proceedings are authorized by CIPA, Fed.R.Crim.P. 16(1), and the
19 common law.⁸ Again, the court is mindful of the argument that denial of access to the
20 FISA and CIPA materials is inconsistent with the adversary process. However, to
21 mitigate the denial of access to the classified materials and to assist the court in its
22 review of CIPA-related materials for purposes of Brady, the First and Fourth
23 Amendments, Fed.R.Crim.P. 16, and the Jencks Act, the court requested, and carefully

24
25 ⁸ “The Government has a compelling interest in protecting both the secrecy of
26 information important to our national security and the appearance of confidentiality so
27 essential to the effective operation of our foreign intelligence service.” CIA v. Sims,
28 471 U.S. 159, 175 (1985). To that end, CIPA Section 4 expressly authorizes the United
States to submit an ex parte motion seeking in camera review of classified information
that may be discoverable in a federal criminal case. 18 U.S.C. App. III § 4. The Ninth
Circuit has endorsed the ex parte proceedings as an appropriate means of reviewing
classified information under CIPA § 4. United States v. Klimavicius-Viloria, 144 F.3d
1249 (9th Cir. 1998).

1 considered, Defendants' jointly submitted sealed memorandum identifying seven broad
2 defense theories as well as specific evidence sought to be discovered in the
3 Government's CIPA §4 submissions. (Ct. Dkt 133-35). Ultimately, for the reasons
4 set forth in the previously filed sealed CIPA orders, the court concluded that certain
5 materials were not helpful to the defense (either because the materials were not relevant
6 or cumulative to other materials already produced to Defendants) and, as to those
7 relevant and helpful statements, the court ordered the Government to provide
8 substituted statements that conveyed the material substance of those statements.

9 Accordingly, the court declines to order the Government to produce FISA- and
10 CIPA- related materials to Defendants.

11 Discovery-Related Issues

12 Defendants argue that the Government seized items (intercepted conversations
13 and telephony metadata) from Defendant Moalin but did not produce them in discovery
14 as required by Fed.R.Crim.P 16. The Government responds that it fully complied with
15 its discovery obligations under Rule 16 and that the interceptions and metadata were
16 obtained via third parties and therefore no violation occurred. The court notes that
17 Defendants fail to identify any evidence not produced by the Government pursuant to
18 Rule 16, the Jencks Act, or Brady.


19 Defendants also argue that the Government failed to comply with its obligations
20 under Brady to produce exculpatory information. Among other things, Defendants
21 seek to discover the reasons underlying the conclusion of the 2003 investigation
22 involving Defendant Moalin; evidence that Defendant Moalin's contacts with al
23 Shabaab were indirect, not direct; exculpatory evidence concerning the earlier Anaheim
24 investigation of Defendant Nasir; and exculpatory evidence related to the so-called FIG
25 assessment. The Government responds that it has complied with its obligations under
26 Brady and produced to Defendants all such materials. The court notes that the court
27 has ordered the Government on several occasions - most recently in its January 30,
28 2013 order - to comply with its obligations under Brady. (Ct. Dkt. 273). Based upon

1 the court’s careful review of all materials provided by the Government under FISA and
2 CIPA, as well as the myriad of intercepted communications provided to the defense,
3 the court has no reason to suspect or speculate that the Government may have faltered
4 in its Brady obligations. The current defense requests for further discovery ignore the
5 timing and nature of the involvement of these Defendants which led to their
6 convictions, which, in turn, were supported by strong and compelling evidence. As
7 Defendants fail to identify any discovery or Brady violation by the Government, the
8 court denies the motion for new trial based upon alleged discovery violations.

9 In sum, the court denies the motion for a new trial in its entirety.

10 **IT IS SO ORDERED.**

11 DATED: November 14, 2013



Hon. Jeffrey T. Miller
United States District Judge

12
13 cc: All parties
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28