UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. BASAALY MOALIN; MOHAMED MOHAMED MOHAMUD; ISSA DOREH; AHMED NASIR TAALIL MOHAMUD, Defendants.	CASE NO. 10cr4246 JM ORDER DENYING MOTION FOR NEW TRIAL

Defendants Basaaly Moalin ("Moalin"), Mohamed Mohamed Mohamud ("Mohamud"), Issa Doreh ("Doreh"), and Ahmed Nasir Taalil Mohamud ("Nasir") jointly move for a new trial pursuant to Federal Rule of Criminal Procedure 33. The Government opposes the motion. Having carefully considered the papers submitted, the court record, and the arguments of counsel, the court denies the motion for new trial.

BACKGROUND

The Second Superseding Indictment

Filed on June 8, 2012, the operative Second Superseding Indictment alleges five counts: (1) conspiracy to provide material support to terrorists in violation of 18 U.S.C. §2339A(a); (2) conspiracy to provide material support to a foreign terrorist organization in violation of 18 U.S.C. §2339B(a)(1); (3) conspiracy to launder

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

The FISA Motion

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

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

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

The CIPA Motions

On March 9, 2012, Defendants jointly and preemptively moved to deny the Government's anticipated request for an ex parte and in camera review pursuant to Section 4 of the Classified Information Protection Act ("CIPA"), 18 U.S.C. App. 3 §4. On March 23, 2012, the Government filed a response to Defendants joint motion to (1) deny the ex parte CIPA filing and (2) compel disclosure of the CIPA materials to cleared defense counsel. To assist the court in its review of CIPA-related materials for purposes of Brady, the First and Fourth Amendments, Fed.R.Crim.P. 16, and the Jencks Act, the court requested, and Defendants jointly submitted under seal, a memorandum identifying seven broad defense theories as well as specific evidence sought to be discovered in the Government's CIPA submission. (Ct. Dkt 133-35).

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

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

[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.

Jencks Act. (Ct. Dkt. 279).

The Rule 15 Depositions

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

The Trial

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

Recent Public Disclosures

On June 8, 2013, The Washington Post reported on disclosures made by Edward Snowden, a former NSA contract employee. As described by Defendants, "[t]he 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." (Motion at p.7:12-14). In broad brush, the disclosures revealed the existence of several classified United States surveillance programs and

[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).

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

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

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

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

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

Classified Facts Summary

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

DISCUSSION

Legal Standards

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

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

[3] Al-Shabaab, a violent and brutal militia group, was designated by the U.S. Department of State as a Foreign Terrorist Organization on February 26, 2008. (Ct. 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).

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

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

The Motion

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

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

The NSA Surveillance

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

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

[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.

parties, including co-defendants.

The Fourth Amendment

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

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

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

---

[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."

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

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

information).

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

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

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

Here, when Defendant Moalin used his telephone to communicate with third parties, whether in Somalia or the United States, he had no legitimate expectation of privacy in the telephone numbers dialed. The calls were routed through the communications company and its switching equipment in the ordinary course of business. While Defendant Moalin may have had some degree of a subjective expectation of privacy, that expectation is not "one that society is prepared to recognize as reasonable." Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (quoting Katz, 389 U.S. at 361). Furthermore, where the calls were initiated by third parties, whether from Somalia or other countries, Defendant Moalin's subjective expectation of privacy is even further diminished because Defendant Moalin cannot assert Fourth Amendment principles on behalf of third parties. The court could not locate any authorities, nor do Defendants cite any pertinent authorities, that recognize any expectation of privacy in the receipt of telephone call data from a third party in a foreign country. As in Smith, because the metadata was obtained through communications companies and their switching equipment, Defendant Moalin "cannot claim that his property was invaded or that police intruded into a 'constitutionally protected area.'" 442 U.S. at 741.[6] While technology continues to advance through the implementation of new devices and methods, the legal analysis remains fairly constant: whether "the government violate[d] a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001). For the above stated reasons, Defendant's

[6] As set forth above, Defendant Moalin lacks standing to challenge the metadata 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.

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

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

> [B]ecause the Application at issue here concerns only the production of call detail records or 'telephony metadata' belong to a telephone company, and not the contents of communications, Smith v. Maryland compels the 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.

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

[7] The court declines to reach Defendants' generalized arguments that (1) the 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.

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

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

The First Amendment

Defendants raise a generalized First Amendment challenge. In broad brush, Defendants argue that "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." (Reply at p.15:12-14). Defendants cite no evidence nor provide legal authority to support the proposition that Defendant Moalin's First Amendment rights were violated in any manner.

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

The FISA and CIPA Section 4 Arguments

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

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

of FISA and CIPA.

Renewed Motion to Gain Access to FISA and CIPA Materials

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

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

[8] "The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service." CIA v. Sims, 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).

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

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

Discovery-Related Issues

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

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

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

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

IT IS SO ORDERED.

DATED: November 14, 2013

Hon. Jeffrey T. Miller
United States District Judge

cc: All parties