No._____

IN THE SUPREME COURT OF THE UNITED STATES

═══════════

MOHAMED MOHAMED MOHAMUD, ISSA DOREH and
AHMED NASIR TAALIL MOHAMUD,

Petitioners

v.

UNITED STATES OF AMERICA,

Respondent.

═══════════

PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

═══════════

PETITION FOR A WRIT OF CERTIORARI

David J. Zugman
Burcham & Zugman
402 West Broadway, Suite 1130
San Diego, California 92101
(619) 699-5931
Attorney for M. M. Mohamud
Counsel of Record

Elizabeth Armena Missakian
Law Office of Elizabeth A. Missakian
PO Box 600021
San Diego, CA 92160
619-985-8848
Attorney for Issa Doreh

Benjamin L. Coleman
Coleman & Balogh LLP
1350 Columbia Street, Suite 600
San Diego, California 92101
Telephone: (619) 794-0420
Attorney for Ahmed Nasir Taalil Mohamud

QUESTIONS PRESENTED FOR REVIEW

A jury convicted four Somali men of providing material support to terrorism by sending $10,900 to al-Shabaab. They contested the government's bulk metadata collection used in their case, but the Ninth Circuit ruled that even if it breached the Fourth Amendment, the evidence would not be suppressed. The Ninth Circuit agreed that the Fourth Amendment requires notice to defendants when the prosecution uses surveillance-derived information but found no prejudice to Petitioners from the lack of notice in this case.

This petition presents the following questions for review:

(1) Whether this Court should review the Ninth Circuit's decision to abstain from deciding the Petitioners' Fourth Amendment and statutory challenge to bulk collection of Petitioners' metadata?

(2) Should this Court review the Ninth Circuit's failure to apply the *Chapman v. California*, 386 U. S. 18, 87 S. Ct. 824, 17 L. Ed. 2d 705 (1967), standard of harmlessness beyond a reasonable doubt to Petitioners' constitutional errors?

(3) Did the Ninth Circuit err by conducting an ex parte review to determine if errors were "material" under *Brady v. Maryland*, 373 U.S. 83 (1963), while excluding the security-cleared defense counsel?

(4) Did the Ninth Circuit correctly find sufficient evidence that Issa Doreh knew funds collected in the United States were sent to al-Shabaab?

PARTIES TO THE PROCEEDING

Petitioners Issa Doreh, Mohamed Mohamed Mohamud, and Ahmed Nasir Taalil Mohamud were three defendants in a four-defendant criminal case before the district court and in the appeal before the Ninth Circuit. The fourth defendant/appellant, Basaaly Saeed Moalin, was represented by retained counsel Joshua Dratel before the district court and Ninth Circuit. He is not a party in the instant petition before this Court.

Respondent United States of America was the plaintiff in the district court and the appellee in the Ninth Circuit.

STATEMENT OF RELATED PROCEEDINGS

Counsel for Petitioners are not aware of any related proceedings in state or federal courts, or in this Court, directly related to this case under Supreme Court Rule 14.1(b)(iii).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Constitutional Provisions

Cases

Statutes

Rules

IN THE SUPREME COURT OF THE UNITED STATES

MOHAMED MOHAMED MOHAMUD, ISSA DOREH and
AHMED NASIR TAALIL MOHAMUD,

Petitioners,

v.

UNITED STATES OF AMERICA,

Respondent.

**PETITION FOR WRIT OF CERTIORARI TO
THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

Petitioners Issa Doreh, Mohamed Mohamed Mohamud, and Ahmed Nasir Taalil Mohamud respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

JURISDICTION

The judgment of the court of appeals was entered on September 2, 2020, nearly four years after oral argument. *See* Appendix A: *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020). Four years after that, the Ninth Circuit denied the petition for rehearing or rehearing en banc on February 27, 2025. *See* Appendix B: Denial of the Petition for Rehearing. On May 29, 2025, Justice Kagan granted Petitioners'

request to extend the time to file a petition for certiorari until July 28, 2025. This Court has jurisdiction under 28 U.S.C. § 1254(1).

STATUTORY PROVISIONS INVOLVED

The statutes involved are 18 U.S.C. § 956, 18 U.S.C. § 1956(a)(2)(A), 18 U.S.C. § 1956(h), 18 U.S.C. § 2339A(a), 18 U.S.C. § 2332a(b), 18 U.S.C. § 2339B(a)(1), 18 U.S.C. § 2339B(g)(6), and 50 U.S.C. § 1861. These statutes are set out in the Appendix.

CONSTITUTIONAL PROVISIONS INVOLVED

Petitioners' arguments are based on the Fourth Amendment, the Fifth Amendment, and the Sixth Amendment.

STATEMENT OF THE CASE

The United States charged Petitioners by a Second Superseding Indictment filed on June 8, 2012, which alleged the following:

Count 1: Conspiracy to provide material support to terrorists, in violation of 18 U.S.C. § 956 [conspiracy to kill persons in a foreign country] and 2332a(b) [conspiracy to use a weapon of mass destruction outside of the United States], all in violation of § 2339A(a).

Count 2: Conspiracy to provide material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(g)(6), all in violation of 18 U.S.C. § 2339B(a)(1).

Count 3: Conspiracy to launder monetary instruments, with the intent to provide

material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1), providing material support to terrorists in violation of 18 U.S.C. § 2339A(a); and conspiracy to kill persons in a foreign country, in violation of 18 U.S.C. § 956, all in violation of 18 U.S.C. § 956, all in violation of 18 U.S.C. § 1956(a)(2)(A) and (h).

Count 4: To Moalin only, conspiracy to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a) [Count Four] and providing material support to foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1) and 2 [Count Five].

Count 5: Providing material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1) and (2) on or about April 23, 2008.

(District court docket, *United States v. Moalin*, 10-cr-04246-JM, Southern District of California hereinafter "CR" 147).

The trial commenced on January 28, 2013, and on February 22, 2013, the jury returned guilty verdicts on all counts against all Defendants. (CR 302). Following the Edward Snowden revelations, Petitioners moved for a new trial; the district court heard the motion on November 13, 2013, and denied it by amended order on November 18, 2013. (CR 388). *See* Appendix C.

On April 10, 2014, the Ninth Circuit consolidated appeal numbers 13-50572, 13-50578, 13-50580, and 14-50051. The Ninth Circuit heard the oral argument on November 10, 2016. On September 20, 2020, the Ninth Circuit published *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020); *see* Appendix A. The Petitioners filed

for Ninth Circuit rehearing and petition for rehearing en banc on November 13, 2020. The Respondent filed a petition for rehearing en banc on November 13, 2020, but that petition was denied the same day as untimely. The Respondent subsequently filed a motion to extend time which was granted on December 1, 2020.

On January 15, 2021, the Ninth Circuit ordered Petitioners to file a response to the United States's petition for rehearing en banc, and the government was ordered to file a response to Petitioners' petition for rehearing en banc. Four years later, on February 27, 2025, the Ninth Circuit unanimously voted to deny both parties' petitions for rehearing. A copy of that order is attached as Appendix B. The mandate was issued on March 5, 2025.

REASONS FOR GRANTING THE WRIT

THE NINTH CIRCUIT APPLIED THE WRONG STANDARD OF REVIEW CONCERNING THE GOVERNMENT'S COLLECTION, RETENTION, AND USE OF TELEPHONE METADATA

The Ninth Circuit all but concluded that the mass collection of telephony metadata under 50 U.S.C. §1861 (Section 215 of the USA PATRIOT Act) of the Foreign Intelligence Surveillance Act ("FISA") was unauthorized and likely violated the Fourth Amendment but avoided a making a final merits decision by finding that any error would have been harmless. *United States v. Moalin*, 973 F.3d 977, 992-93, 996 (9th Cir. 2020); Appendix A. The United States did not disclose to Petitioners the method by which it obtained their data, and only after surveillance activities were reported to Congress after trial did the United States inform Petitioners that

Mr. Moalin's data had been collected (along with every other cellphone user). The Ninth Circuit held that any illegality associated with the interception of Mr. Moalin's electronic communications through other surveillance programs which "may have violated the Fourth Amendment" was also harmless error. *Id.* at 100-01.

The Ninth Circuit's refusal to decide the Fourth Amendment issue is in defiance of this Court's precedent regarding metadata, such as historical cell site data, which is protected by the Fourth Amendment. *See Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206 (2018). Given that the telephony metadata at issue in this case is analogous to the cell site data in *Carpenter*, the Ninth Circuit erred by disregarding this precedent and proceeding directly to harmless error. *Id.* at 1001. The Ninth Circuit did not apply the standard of review for constitutional errors and, consequently, did not consider whether these constitutional errors were harmless beyond a reasonable doubt.

Each of Petitioners' arguments had a constitutional dimension so the United States was required to prove beyond a reasonable doubt that the error did not contribute to the verdict. *Chapman v. California*, 386 U. S. 18, 87 S. Ct. 824, 17 L. Ed. 2d 705 (1967). The failure of the prosecution to provide *Brady v. Maryland*, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963), material is a constitutional claim, *United States. v. Moalin*, 973 F.3d at 1001-02. There is a constitutional dimension to Petitioners' attempt to present exculpatory evidence in the testimony by defense witness Halima Ibrahim. *Id.* at 1002-03. The district court's refusal to order the

government to provide safe passage to a defense witness (Farah Shidane, a/k/a "Farah Yare") for purposes of a deposition overseas pursuant to Federal Rule of Criminal Procedure Rule 15. *Id.* at 1003-04. Finally, the trial court's failure to prohibit the government from presenting "expert" testimony about the notorious "Black Hawk Down" incident in Mogadishu, Somalia in 1993, in which eighteen U.S. soldiers were killed. *Id.* at 1005-06. This is a constitutional issue under the recently decided *Andrew v. White*, 604 U.S. ___ (2025), 145 S. Ct. 75, 78 (2025) (per curiam).

In *Andrew*, this Court ruled that introducing highly prejudicial, irrelevant evidence, such as gendered and inflammatory references to the defendant's personal life, can violate due process by making a trial fundamentally unfair. *Andrew v. White*, 145 S. Ct. at 78 ("By the time of Andrew's trial, this Court had made clear that when 'evidence is introduced that is so unduly prejudicial that it renders the trial fundamentally unfair, the Due Process Clause of the Fourteenth Amendment provides a mechanism for relief.' *Payne v. Tennessee*, 501 U. S. 808, 825, 111 S. Ct. 2597, 115 L. Ed. 2d 720 (1991).") Petitioners argued that the "Black Hawk Down" testimony, referencing the 1993 killing of eighteen U.S. soldiers and a Hollywood blockbuster, was similarly prejudicial and irrelevant, serving only to inflame the jury's emotions. At least the relationship between Ms. Andrew and her husband was a factual issue in the trial; the "Black Hawk Down" testimony had no tie to any fact presented at trial and the sole purpose of the testimony was to portray Petitioners

as aligned with enemies and terrorists who killed U.S. soldiers.

A. The Errors Below Relating to FISA

The Ninth Circuit correctly held that "the telephony metadata collection program exceeded the scope of Congress's authorization in section 1861 and therefore violated that section of FISA." *Id.* at 996 (citing *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 826 (2d Cir. 2015)). The Ninth Circuit went on to observe that the violation of the statute also likely violated the Fourth Amendment, but instead of following the argument through, the Ninth Circuit shortcutted to harmless error and found that any illegalities did not taint the government's collection of evidence, including its subsequent electronic surveillance conducted pursuant to FISA:

> [c]ontrary to defendants' assumption, the government maintains that Moalin's metadata "did not and was not necessary to support the requisite probable cause showing" for the Subchapter I application in this case. Our review of the classified record confirms this representation.

977 F.3d at 997.

The Ninth Circuit also noted that:

> [even] if we were to apply a "fruit of the poisonous tree" analysis, *see Wong Sun* [*v. United States*, 371 U.S. 471, 487-488 (1963)], we would conclude, based on our careful review of the classified FISA applications and related information, that the FISA wiretap evidence was not the fruit of the unlawful metadata collection.

Id. at 993 (citing *Wong Sun,* 371 U.S. at 488).

After secretly determining that the government's illegal surveillance was neither the exclusive nor essential justification for the wiretap against Mr. Moalin, the Ninth Circuit chose not to address the potential Fourth Amendment violation directly. However, following a review of Petitioners' briefing, the court observed that "for all these reasons, defendants' Fourth Amendment argument has considerable force." *Id.*, at 992. The Ninth Circuit added it did "not come to rest as to whether the discontinued metadata program violated the Fourth Amendment because even if it did, suppression would not be warranted on the facts of this case." *Id.* at 992-93, (citing *United States v. Ankeny*, 502 F.3d 829, 836-37 (9th Cir. 2007)).

With respect to whether appellants were entitled to notice of the FISA collection, the Ninth Circuit concluded that

> assuming without deciding that the government should have provided notice of the metadata collection to defendants, the government's failure to do so did not prejudice defendants. Defendants learned of the metadata collection, albeit in an unusual way, in time to challenge the legality of the program in their motion for a new trial and on appeal.

Id., at 1001 (citing *United States v. Mohamud*, 843 F.3d 420, 436 (9th Cir. 2016)).

Appellants also argued that there were other, warrantless unlawful electronic surveillance programs which were used against them, but the Ninth Circuit again relied on the ex parte evidence to reject the claim: "[b]ased on our careful review of the classified record, we are satisfied that any lack of notice, assuming such notice was required, did not prejudice defendants." *Id.* The Ninth

Circuit ruled that the government's violation of FISA §1861 was harmless, the government's potential violation of the Fourth Amendment was harmless, and the government's failure to provide Appellants the required notice under the Fourth Amendment was harmless but did not publicly say how.

In each instance the Ninth Circuit failed to articulate the proper standard for an error of constitutional magnitude as required for the potential Fourth Amendment violation: that the government establish the error's harmlessness beyond a reasonable doubt. *See Neder v. United States*, 527 U.S. 1, 15 (1999) (*quoting Chapman v. California,* 386 U.S. 18, 24 (1967)); *see also Gautt v. Lewis*, 489 F.3d 993, 1014-16 (9th Cir. 2007).

This case presents an ideal vehicle to resolve an increasingly recurring question: whether courts may avoid enforcing the Fourth Amendment in the face of a clear constitutional error by using harmless error (and applying it incorrectly). The Ninth Circuit did not apply the *Chapman v. California*, 386 U.S. 18 (1967), standard by placing the burden on the government to prove harmlessness beyond a reasonable doubt. *See Neder v. United States*, 527 U.S. 1, 7-8 (1999); *Sullivan v. Louisiana*, 508 U.S. 275, 279 (1993); *Arizona v. Fulminante*, 499 U.S. 279, 295-96 (1991).

The Ninth Circuit treated constitutional errors—including potentially unlawful surveillance under FISA and the Fourth Amendment, and the suppression of exculpatory evidence under *Brady v. Maryland*, 373 U.S. 83 (1963)—as harmless

based on a silent record and with ex parte review. The phrase "harmless beyond a reasonable doubt" appears nowhere in the Ninth Circuit's published opinion and that failure directly conflicts with multiple precedents of this Court. Nearly four decades ago in *Satterwhite v. Texas*, 486 U.S. 249, 258-59 (1988), this Court reversed because the lower court failed to apply *Chapman* and instead relied on the sufficiency of the remaining evidence—an impermissible substitute for the harmless-beyond-a-reasonable-doubt standard. In *Yates v. Evatt*, 500 U.S. 391, 402-03 (1991), the Court reversed because a state court improperly analyzed harmlessness in asking whether the jury could have convicted absent the error, rather than whether the error contributed to the verdict. *O'Neal v. McAninch*, 513 U.S. 432, 438 (1995), reiterated that when a reviewing court is in "grave doubt" as to whether an error affected the verdict, the conviction cannot stand.

This precedent has not been questioned or undercut in the subsequent three decades. But in *Moalin,* the Ninth Circuit conducted its own ex parte review of classified material and concluded—without adversarial testing and without applying *Chapman*—that unlawful surveillance and the suppression of exculpatory materials and exclusion of exculpatory testimony did not prejudice the defense. These are precisely the kinds of determinations this Court has warned against: ones made without full adversarial process and without the government proving harmlessness to the required constitutional standard.

This Court should grant review to clarify that when constitutional violations are established appellate courts should not sidestep to *Chapman* by omitting it, softening it, or replacing it with a silent record review.

Further, the Fourth Amendment issue is one that this Court should speak to because the law is supposed to care a great deal that the officers are acting in good faith. *See Davis v. United States*, 564 U.S. 229, 131 S. Ct. 2419 (2011) (if police are acting in good-faith and under formerly binding precedent, then the Fourth Amendment does not require suppression.) The police conduct here is not in good-faith as in being based on any previously accepted mode of surveillance. Instead, this was a secret data harvesting program that the United States was using to prosecute Petitioners. This case involves a secret record where the defendants never get to look at the evidence that supposedly dooms their constitutional claims. The Ninth Circuit's refusal to decide the illegality that was plainly before it calls for this Court's correction.

The United States Constitution has a right to privacy and the Fourth Amendment is one manifestation thereof. The law requires that before seizure, search, and bulk retention of private metadata, the government is required to get a warrant from a neutral magistrate before it seizes and mines the undifferentiated metadata of hundreds of millions of people to investigate them. The Founders were in favor of placing "'obstacles in the way of a too permeating police surveillance.' *United States v. Di Re*, 332 U. S. 581, 595, 68 S. Ct. 222, 92 L. Ed. 210 (1948)."

Carpenter v. United States, 585 U.S. at 305, 138 S. Ct. at 2214. The United States is not a surveillance state and the officers that enacted this program and hid it should be reminded of that.

In *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 2485 (2014), this Court recognized that cell phone data, due to its vast scope and intimate detail, implicates profound privacy concerns, holding that warrantless searches of such data violate the Fourth Amendment. The bulk telephony metadata collection under FISA § 1861, as in this case, *Moalin*, 973 F.3d at 992-93, similarly amasses sensitive personal information, enabling an unprecedented level of intrusion into private lives, as cautioned in *Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206, 2217 (2018) (holding that historical cell-site data constitutes a Fourth Amendment search). Such programs, conducted in secrecy and without adequate judicial oversight, erode the constitutional protections against a surveillance state, as this Court warned in *Katz v. United States*, 389 U.S. 347, 351 (1967) (establishing privacy as a core Fourth Amendment value), and *United States v. Jones*, 565 U.S. 400, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (noting that unchecked surveillance chills democratic freedoms). The Court should grant certiorari to reaffirm that the Fourth Amendment forbids such blanket surveillance and provide lower courts with clearer guidance about safeguarding individual privacy.

Judged by the proper standard, and, as set forth in section C below, especially with the participation of security-cleared trial court counsel in identifying

the impact of the errors, it is respectfully submitted that the Ninth Circuit would not have affirmed Appellants' convictions. Accordingly, Petitioners ask this Court to grant review in this case to decide whether the multiple errors related to the FISA interceptions and evidence were harmless beyond a reasonable doubt.

B. The *Brady* and Constitutional Trial Evidentiary Errors Below

In denying Appellants' *Brady* claim, *see* 973 F.3d at 1001-02, the Ninth Circuit concluded, after its ex parte review of classified information provided by the government, that any non-disclosure to Appellants was not "material," and therefore did not constitute a *Brady* violation. However, the information referred to in the intelligence assessment and the linguist's memoranda, which likely would have negated any criminal intent on Mr. Moalin's part (and therefore the intent of the other defendants as well), and established that his contacts with Somalia were widespread and not intended to support al-Shabaab, but instead were directed at humanitarian relief in Somalia and his own commercial interests there, was decidedly material.

The Ninth Circuit failed to apply the correct standard of review to constitutional dimensions of the evidentiary arguments of Petitioners. For example, regarding the District Court's preclusion of certain exculpatory testimony by defense witness Halim Ibrahim, the Ninth Circuit stated it could not "say that the exclusion of Ibrahim's testimony regarding the 2009 conference 'more likely than

not affected the verdict.'" *Id.* at 1003 (quoting *United States v. Pang*, 362 F.3d 1187, 1192 (9th Cir. 2004)). That is not the harmless beyond a reasonable doubt standard.

Similarly, with respect to the denial of safe passage for Mr. Shidane, the Ninth Circuit stated that "[e]ven if the district court did abuse its discretion, any error, in denying either defendants' request for 'safe passage' or their request to depose Shidane by video, was harmless." *Id.* at 1005. Regarding the government expert's testimony about the "Black Hawk Down" incident, *see id.*, the Ninth Circuit decided that "even if the district court did abuse its discretion in admitting the testimony, the error was harmless." *Id.* (*citing Pang*, 362 F.3d at 1192).[1]

Ultimately, considering the claim of cumulative error, the Ninth Circuit answered that "[t]o the extent we have found the claimed errors of the district court harmless, 'we conclude that the cumulative effect of such claimed errors is also harmless because it is more probable than not that, taken together, they did not materially affect the verdict.'" *Id.* at 1006 (quoting *United States v. Fernandez*, 388 F.3d 1199, 1256-57 (9th Cir. 2004)).

Here, while each of the errors listed above includes an evidentiary aspect based on the Federal Rules of Evidence, each also clearly presents a constitutional

---

[1] In so doing, the Ninth Circuit stated that "[t]he expert's testimony was not tied to defendants or to al-Shabaab in any way and was therefore unlikely to have prejudiced the jury against defendants." 973 F.3d at 1005. The testimony was about Somali men hunting down and killing eighteen U.S. soldiers. And the defendants were Somali men who were being accused of supporting the terrorists in Somalia. There is no reason for this testimony except to connect Petitioners to the malefactors who killed our troops in *Black Hawk Down*.

issue: respectively, the Fifth Amendment Due Process right to disclosure of exculpatory evidence, the Sixth Amendment right to present testimony (with the Fifth Amendment Due Process right to present a defense), the Sixth Amendment right to call witnesses; and the Fifth Amendment Due Process right to a fair trial free of undue prejudice and aggregate evidentiary error.

The phrase "harmless beyond a reasonable doubt" does not appear at all in the Ninth Circuit's opinion, despite the four instances – including whether the accumulation of error denied appellants a fair trial – in which the Ninth Circuit considered a potential error harmless. An error "cannot be harmless where it prevents the defendant from providing an evidentiary basis for his defense." *United States v. Saenz*, 179 F.3d 686, 689 (9th Cir. 1999). Yet that was the case with each of the errors enumerated above, and surely all of them in combination. Also, when a defendant is not able to proffer a full and fair defense, Fifth and Sixth Amendments rights to present a defense are implicated, and the court must engage in the stricter harmless error analysis to ensure that the "error complained of did not contribute to the verdict obtained.'" *Neder*, 527 U.S. at 15, quoting *Chapman*, 386 U.S. at 24.

In *Andrew v. White*, this Court reaffirmed that evidentiary errors could rise to a constitutional violation when they undermine fundamental fairness, as when irrelevant, inflammatory evidence (such as the "Black Hawk Down" testimony here) distorts the fact-finding process. 604 U.S. at ___ (citing *Payne v. Tennessee*, 501 U.S. 808 (1991); *Estelle v. McGuire*, 502 U.S. 62 (1991)). The Ninth Circuit's failure

to apply *Chapman* to this error, as well as to the Fourth Amendment and *Brady* violations, mirrors the error in *Andrew*, where the lower court insufficiently scrutinized the prejudicial impact of evidence under a constitutional lens.

C. The FISA and Brady Issues Could Not Adequately Be Decided Ex Parte

1. Ex Parte proceedings are inadequate

In deciding that the violations of §1861 and the potential Fourth Amendment violations did not taint the FISA-generated evidence, the Ninth Circuit relied wholly on an ex parte review of the classified record. The same is true for the Ninth Circuit's determination of Appellants' *Brady* issue. However, it is respectfully submitted that ex parte examination of the record– particularly when each Appellant below had trial counsel who possessed the requisite security clearance to review the classified information at issue – does not provide the Court sufficient basis for a decision that affirms convictions and long prison sentences. It is axiomatic that ex parte proceedings deprive the Court of the ability to make an accurate determination. *See Alderman v. United States*, 394 U.S. 165, 168, 180-85 (1969) (refusing "to accept the ex parte determination of relevance by the Department of Justice in lieu of adversary proceedings in the District Court"). Ex parte proceedings also deny a criminal defendant the Fifth Amendment guarantee of Due Process, and the Sixth Amendment right to confrontation.

It is particularly insufficient on appeal, when the intricacies of the impact of certain information on the issues may not be apparent from the cold record. The

necessity of that perspective renders defense counsel's contribution indispensable. Indeed, the direction in *Neder* that a Court must conduct a "thorough examination of the record" 527 U.S. at 19, before concluding that the constitutional error was harmless is impossible to achieve without input from one party to the case (and in particular the party that bears the full brunt of a contrary holding based on ex parte review).

2. The Ninth Circuit's conclusion is directly contradicted by the public record

These general principles are even more pertinent in the context of Petitioners' case, where the Ninth Circuit's ex parte review led to conclusions which are directly contradicted by public statements from high-ranking officials, undermining the reliability of the judicial process and implicating constitutional fairness. For example, regarding the FISA issues, the Ninth Circuit acknowledged that the FBI's Deputy Director publicly testified before Congress in a manner entirely contrary to the Ninth Circuit's conclusion that the unlawful metadata collection did not taint the FISA wiretap evidence. *See United States v. Moalin*, 973 F.3d at 997-98. The Deputy Director's testimony suggested that the metadata collection was integral to establishing probable cause for the FISA surveillance, directly challenging the Ninth Circuit's assertion, based on its ex parte review, that "Moalin's metadata 'did not and was not necessary to support the requisite probable cause showing'" for the FISA wiretap application. *Id.* at 997.

The Ninth Circuit dismissed this contradiction by stating that "if the statements of public officials created a contrary impression, that impression is inconsistent with the facts presented in the classified record." *Id.* at 993 (footnote omitted). This dismissal without adversarial input is particularly troubling given the availability of security-cleared trial court defense counsel who could have tested the classified record's veracity against the public testimony, potentially revealing discrepancies critical to the Fourth Amendment analysis. The reliance on ex parte review to resolve a constitutional issue—without allowing defense counsel to challenge the government's representations—deprived Petitioners of a fair opportunity to contest evidence central to their convictions, implicating their Fifth Amendment due process rights.

The Deputy Director's public statements, made under oath before Congress, suggested that the metadata collection was a critical component of the surveillance framework, directly undermining the Ninth Circuit's ex parte conclusion that the metadata was irrelevant to the FISA wiretap's probable cause. This discrepancy creates, at minimum, "virtual equipoise" as to the harmlessness of the Fourth Amendment violation, requiring reversal under this Court's precedent. *See O'Neal v. McAninch*, 513 U.S. 432, 435 (1995). Yet, the Ninth Circuit resolved this critical issue without input from security-cleared defense counsel, who could have probed the classified record to clarify whether the metadata collection indeed influenced the FISA application, as the Deputy Director's testimony implied.

This Court has long emphasized that ex parte proceedings are inadequate for resolving complex factual disputes, particularly when constitutional rights are at stake. *See Alderman,* 394 U.S. at 181-84. Here, the Ninth Circuit's ex parte dismissal of a potential Fourth Amendment violation, despite conflicting public testimony, similarly risks a miscarriage of justice by foreclosing the adversarial process necessary to protect Petitioners' constitutional rights.

The public statements at issue at the very least create the necessity for an evidentiary hearing. This is the grave doubt circumstance in which "a judge 'feels himself in virtual equipoise as to the harmlessness of the error' and has 'grave doubt' about whether an error affected a jury [substantially and injuriously], the judge must treat the error as if it did so.'" *Merolillo v. Yates*, 663 F.3d 444, 454 (9th Cir. 2011) (quoting *O'Neal v. McAninch*, 513 U.S. 432, 435 (1995)) (*quoting Kotteakos v. United States*, 328 U.S. 750, 765 (1946)) (brackets in *Merolillo*). Sworn Congressional testimony by the FBI's Deputy Director should satisfy the "virtual equipoise" required for grave doubt.

3. With the clear contradiction between the statements of a high government official before Congress, security-cleared counsel should have been allowed to review the evidence

The Ninth Circuit maintained that while "defendants contend the government was required to produce any favorable, material evidence relating to the FISA surveillance or to the previously terminated investigation of Moalin[,]" 973 F.3d at 1002, based on the Ninth Circuit's "review of the classified record and of

the district court's extensive sealed orders covering *Brady* issues, neither the classified FISA materials nor the file concerning the previously terminated investigation of Moalin contained favorable, material information." *Id.* Such a conclusive determination could not possibly be reached with any confidence without the contribution of security-cleared defense counsel providing the requisite defense perspective – the whole objective of the adversary process's quest for accurate, just, and fair process and results. Conversely, granting security-cleared defense counsel access to the classified record the Ninth Circuit reviewed would not only satisfy constitutional imperatives, but it would also ultimately provide the Court with the adversarial testing which is required for finding truth. *Polk Cnty. v. Dodson*, 454 U.S. 312, 318, 102 S. Ct. 445, 450 (1981) ("The system assumes that adversarial testing will ultimately advance the public interest in truth and fairness.") There is a strong case for reaching the opposite conclusion from that of the Ninth Circuit, and with the benefit of adversarial testing by cleared defense counsel, the Court could determine that the FISA-obtained evidence was unlawfully acquired or materially tainted, warranting its suppression, the vacatur of Petitioners' convictions, and the granting of a new trial consistent with due process.

D. The Evidence Was Insufficient to Support the Convictions of Petitioner Doreh

Issa Doreh was charged in Count 1 of the Second Superseding Indictment with conspiracy to provide material support to terrorists in violation of 18 U.S.C. §

2339A(a); Count 2, conspiracy to provide material support to a Foreign Terrorist Organization in violation of 18 U.S.C. § 2339B(a)(1); Count 3, conspiracy to launder monetary instruments in violation of 18 U.S.C. § 1956(a)(2)(A) and (h); and Count 5, providing material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1) and (2). *United States v. Moalin*, 973 F.3d at 1006.

Nowhere in the Opinion does the Ninth Circuit find there was evidence that petitioner Doreh was aware of the identity of Shikhalow as Aden Ayrow, let alone evidence of knowledge that monies sent to Somalia were for the purpose of supporting Shikhalow or al Shabaab. The fact that transcripts may indicate Doreh was aware of Shikhalow's death on May 1, 2008, in a U.S. missile strike did not in any way prove Doreh knew the person codefendant Moalin was talking to on phone calls was in fact Aden Ayrow. The entire set of transcripts relied on in the Opinion suffers from the same infirmity – a lack of evidence that Doreh knew monies collected in the United States were for the purpose of supporting Ayrow and/or al Shabaab.

To convict Issa Doreh on Count 1, the reviewing court had to find the government had proven (1) that Doreh entered into a conspiracy; (2) that the objective thereof was to provide material support or resources to al-Shabaab; and (3) that Doreh then knew and intended that such support or resources would be used in preparation for, or in carrying out, a separate conspiracy to murder, kidnap, or maim outside of the United States. *See* 18 U.S.C. § 2339A; *United States v. Hassan*,

742 F.3d 104 (4th Cir. 2014); *United States v. Chandia*, 514 F.3d 365, 372 (4th Cir. 2008). With respect to the first element, the government was obliged to prove a conspiracy — that is, an agreement between two or more people to engage in illegal activity. *See United States v. Burgos,* 94 F.3d 849, 857-58 (4th Cir. 1996) (en banc). Issa Doreh's involvement in such a conspiracy would be adequately demonstrated if the evidence showed "a slight connection between [him] and the conspiracy." *See United States v. Kellam*, 568 F.3d 125, 139 (4th Cir. 2009) (internal quotation marks omitted).

The "existence of a tacit or mutual understanding is sufficient to establish a conspiratorial agreement, and proof of such an agreement need not be direct — it may be inferred from circumstantial evidence." *Id.* The Opinion sets forth no such evidence, tacit or otherwise, that Issa Doreh had entered into an agreement with anyone to engage in illegal activity. The government never proved that Doreh ever supported al-Shabaab or Aden Ayrow. It should be noted here that the government admitted it did not know and could not prove that the person identified as Shikhalow (on any intercepted calls, including the 11 calls Issa Doreh participated in) was in fact Aden Ayrow. The Opinion acknowledges as much at page 54: "While the transcripts do not include direct conversations between Doreh and Shikhalow, they describe Doreh's involvement with Moalin and others in transferring funds from San Diego to Shikhalow's organization in Somalia." While the transcripts do

show Doreh's very limited involvement in the transfer of funds, they do not show knowledge that the funds were to Shikhalow or to al-Shabaab.

Even if Issa Doreh was found to have supported an insurgency against Ethiopia, there was no proof that that insurgency was either al-Shabaab or a terrorist group let alone a group designated by this Country as an FTO. As to the second element of the conspiracy charged in Count 1, "material support or resources" is defined as "any property, tangible or intangible, or service," including "currency," "training," "expert advice or assistance," "weapons," or "personnel." 18 U.S.C. § 2339A(b)(1). The third element required the government to establish that Issa Doreh acted "with the knowledge or intent" that such material support or resources would be used to commit a specific violent crime. *United States v. Stewart*, 590 F.3d 93, 117-18 (2d Cir. 2009) ("Stewart and Yousry knew that their actions provided material support to a conspiracy to end the cease-fire and thereby unloose deadly acts of terrorism by al-Gama'a and others, then they were on notice that what they were doing was prohibited by a statute that criminalizes the provision of material support "knowing or intending that [such support is] to be used in preparation for, or in carrying out," criminal actions. 18 U.S.C. § 2339A.")

Under the instructions given by the district court as to Count 1, the government had to prove beyond a reasonable doubt for purpose of Count 1 that Issa Doreh intended to commit murder and/or he intended to provide material support for a weapon of mass destruction. As to either, mere recklessness or

knowledge would not satisfy the government's burden. *See United States v. Chhun,* 744 F.3d 1110, 1117 (9th Cir. 2014). When viewed in the light most favorable to the government, the evidence was insufficient to show that Issa Doreh had the requisite mens rea of intent to commit the offenses in Count 1, namely murder and/or to provide a weapon of mass destruction.

Similarly, as to Count 2 which alleged a conspiracy to provide material support to a foreign terrorist organization in violation of § 2339B, the government had to prove Doreh became a member of the conspiracy charged in Count 2 while knowing of its unlawful object and intending to help accomplish it. Again, the evidence was not just insufficient; it was absent because there was no evidence to support a finding that Issa Doreh knew of any unlawful object nor that he intended to accomplish an unlawful object by doing his job which was to act as a minor player in the Shidaal Express. As the government well knows, when Basally Moalin asked Issa Doreh on April 23, 2008, for the name of the sender, Doreh said, "Well he is not here now; he is the one who sent it, I can't log into the website; I don't have an account, I don't send money, you know." When asked who sends the money, Doreh says "Abdirizak is the person who sends the money." (Exhibit 159; 6RT 1059.)

Count 3 required that Issa Doreh knew of the unlawful purpose of a conspiracy to launder money and intended to accomplish the unlawful purpose. Again, the evidence presented by the government was that Doreh was a clerk in the Shidaal Express; a person who had no access to the actual mechanics of money

transfers. The government knew this not only on the basis of its investigation and indictment of the owner of the Shidaal Express (Abdirizak Hussein) but because of Doreh's statements on the intercepted calls.

Again, as is true in the case of Counts 1-3, a necessary element of Count 5 in the case of Doreh was that he "knowingly provided material support or resources to al-Shabaab" and there was no evidence to support such an allegation.

Contrary to the government's theory and argument at trial, evidence presented to the jury proved Issa Doreh was not only not able on his own to grant discounts or to transmit monies from San Diego to Somalia, every transaction was approved not by him but by Donnah Locsin. (4RT 761.) Additionally, during a call on April 23, 2008 (Exhibit 159; 6RT1059), Moalin asks Doreh about the name of a sender on a particular transfer and Doreh says "he" (meaning Abdirizak) is not here now and "he" is the one who sent it and that he (Doreh) can't log into the website, "I don't have an account, I don't send money, you know." (*Id.* p. 2.) Abdisalam Guled testified that money was sent to Somalia from the diaspora through a hawala and that when money is sent through a hawala by a recognized charity that has an account with the hawala, normally a fee is not charged. If it is not recognized as charity, but the promise of charity sending of this money (outreach or hospital), the fee is minimized but still charged. (12RT 1687).

Furthermore, contrary to the government's contention and argument to jurors, discounts were made by the owner, Mohamud Ahmed and his business

manager, Abdirizak Hussein, not by Issa Doreh. The government knew full well that this was true as reflected in the separate indictment (Southern District of California, Case No. 13CR1514-JM, filed on April 23, 2013) in which Abdiaziz Hussein (aka Abdiaziz Hussen, aka Abdirizak) was alleged in Count 1 to be "Shidaal's manager and responsible for daily operations from 2007 until approximately November 2009. Of particular interest is the fact that overt acts relating to transfers on April 23, 2008, and April 25, 2008, mirrored those in Doreh's indictment as caused by Moalin, Issa Doreh and Mohamud Mohamed, however the government alleged in 13CR1514 that these transfers were caused by Hussein. (CR 147; ER 7-8). In fact, Issa Doreh did not have access to the money wiring equipment; he did not have an ID and password to enter the system, and he certainly was not, as argued by the government, in a position to waive fees or discounts. The government's argument at page (13RT 1974) of its rebuttal argument, that Moalin told someone named Shikhalow that Issa Doreh could waive the fee does not make it true.

The Second Superseding indictment states, in Overt Act 11, "on or about July 15, 2008, defendant Doreh caused the transfer of $2,280 from San Diego, California to Somalia." (ER 8). The government argued the same at the time of trial. Not only did the government know that Doreh did not have the access, authority or power to transfer money to Somalia, the government also misrepresented the transfer of $2,280 as personally sent by him. That money, as the government knows well from

its translation of the intercepted calls on July 8 and 21, 2008, was sent to Farah Shidane who was not affiliated with al-Shabaab but was involved in humanitarian relief. While presenting the fact of the transactions during trial, the government concealed from jurors the actual intercepted calls which would have shown the recipient was Farah Shidane who worked to provide humanitarian relief in Somali. His efforts were completely opposed by al-Shabaab. The fact that funds were sent from the diaspora to Somalia for humanitarian relief is evidenced in a call on February 18, 2008, presented as a defense exhibit. In that call, which is between Moalin and Sahal, who had been mentioned in the first call as the guy that runs the orphanage, Issa Doreh is introduced to Sahal as the guy that runs the orphanage. Government witness Bryden also testified to the money sent by members of the diaspora to Somalia. (3RT 440).

On a call at 04:56:39 UTC on July 2, 2008, between Farah Shidane, Moalin and Mohamed Mohamud, the three have a lengthy discussion of fighting, however the attack by Farah Shidane and his people were of Ethiopians. He makes clear in this conversation when he says "The situation changed and our army was forced to follow them and attack the Ethiopians from the rear. This was the first time in one year of fighting that we attacked them from behind while they were in retreat." (Exhibit 182 at p. 6-7; 6RT 1090). If the government is correct, certainly not conceded by Doreh, that references to "the youth" were in fact a reference to al-Shabaab, the distinction between what Farah Shidane's men were doing and what

"the youth" were doing is great. Farah Shidane says in that same call that "The Youth fought for three minutes and left. That resulted in some of our brothers being exposed to danger and the enemy came around and killed some of our men, like professor Aspro and others, although they fought well. Furthermore, other groups of fighters joined the fight, and it continued for four hours without stop. (*Id.*) Farah Shidane says, in response to Sheik Mohamed's question, that the Somali Islamic Liberation Organization and his (Shidane's group) are the same. (*Id.* at 4 of 7). At no time does Shidane or anyone else say that the Somali Islamic Liberation Organization is the same as or affiliated with al-Shabaab.

With respect to the Opinion's conclusion that Doreh caused the transfer of $2,280 from San Diego to Somalia on July 15, 2008 (Count 1, Overt Act 11(n), there were four calls on July 8, only three of which (Exhibits 183, 184 and 185; 5RT 886, 889, 6RT 1117) were introduced into evidence by the government. Exhibit 184 is a call on July 8, 2008, from Moalin and Doreh to Mohamed Abdi Hassan Yusuf. This call clearly concerns monies collected were intended to be sent to the students of the Koran School, the people and the orphans. He continues to say that the money has been divided into three Koran schools. Hassan says he and the children don't have anything to transport the grain and no means of transportation for these books. (Exhibit 184 at p 7).

In a call on July 8, 2008, from Moalin to Doreh, when asked by Moalin if Doreh sent the money, Doreh says "I gave the money to Mohamud. I didn't send the

money." (6RT 1117). At the time of this call, Mohamud Ahmed was the owner of Shidaal Express.

At 03:51:48 UTC on July 21, 2008, Moalin spoke on a call with Farah Shidane who said he had received $1,030 at one time and $1,250 at another time. These funds are the monies the government attributed to Issa Doreh as going to terrorists when in fact they were clearly for Farah Shidane who was neither al-Shabaab nor a terrorist.

There was no evidence to support the allegation that Issa Doreh "caused the transfer of $2,280 from San Diego, California to Somalia." In fact, in a call on July 22, 2008, at 17:25:20 between Moalin and Issa Doreh, Moalin says the transfer belonged to the children and Doreh clearly says "Right, actually I was not present and the man I delegated was absent for awhile. He was not even available yesterday when they did the inquiry." (Exhibit TT-196A; 10RT 1511). As the evidence at trial established, Farah Shidane was involved in humanitarian works. In fact, money from the diaspora for humanitarian work is a threat through the government's intercepted calls. As early as December 2007, there were discussions about fund-raising for orphans, for a school called ILEYS and mention of a man by the name of Sahal who ran an orphanage.

Additionally, not only did the government never prove that the Shikhalow referenced on the calls was Aden Ayrow, but there was also no evidence that there was a relationship between Issa Doreh and Aden Ayrow or al-Shabaab or that

Doreh knew who Ayrow was. Even more significant is the fact that at no time did the government prove, in all of its recorded intercepts that Issa Doreh ever heard the name Shikhalow or Aden Ayrow. Even if Doreh knew Moalin was sending money to Somalia, there was no evidence that he knew this money was being sent to either Ayrow or al-Shabaab or to a terrorist organization or that he did anything other than his job as a clerk at the Shidaal Express – namely to send money from members of the diaspora to Somalia.

In the calls between Issa Doreh and Basaaly Moalin which were introduced at trial, Moalin never mentioned the name Shikhalow as claimed by the government. Moalin would refer to the "cleric" and there is no evidence that Issa Doreh knew the "cleric" was or that it was a reference to Ayrow rather than another cleric. This follows from a probability law: "'When you hear hoofbeats, think horses, not zebras.' The point is that when trying to explain an unknown phenomenon, it's usually sensible to look first to the familiar and only later to the exotic." *Vance v. Rumsfeld*, 701 F.3d 193, 220 (7th Cir. 2012)

The parties stipulated and agreed to the following facts: "[I]n early to mid 2008, one, money collected for the Ayr subclan was given to individuals, including Abukar Suryare, AKA Abukar Mohamed, and Farah Shidane, who were associated with the ILEYS charity; two, money collected by men in Guraceel on behalf of the Ayr subclan was given to a group that was not al-Shabaab; three, there was a (12RT 1732) dispute between al-Shabaab, the Ayr clan, and ILEYS over the

administration of the Galgaduud region. Four, members of the ILEYS charity and the Ayr subclan, including Abukar Suryare, were opposed to al-Shabaab and were Ayrow's enemies." (12RT 1732-1733).

The intercepted calls in which he participated failed to establish that Doreh knew who Shikhalow was, or that he supported al-Shabaab or knew monies were being sent to al-Shabaab, or that he supported terrorism. There is no dispute that monies transferred on July 15, 2008, totaling $2,280 were sent not to al-Shabaab but to Farad Shidane and there is also no dispute that Farah Shidane was not affiliated with al-Shabaab. Government witnesses, as well as Doreh's own words on intercepted calls, proved he was merely a clerk at the Shidaal Express and had no authority over transfers, including no authority over discounts of fees. It must be remembered, according to the government's own expert Bryden, that it was not merely al-Shabaab versus the TFG; it was a broad-based insurgency. In the context of Somali culture, the concept of insurgency refers to a group of regional, clan-based, civil societies that exist autonomously. Government witness Bryden characterized the organizational structure of Somali society as a "segmentary lineage system." (3RT 442-443).

The citations to transcripts in the Opinion failed to prove that any calls involving Issa Doreh supported al-Shabaab or terrorism in any way. The calls must be viewed in the context of the slaughter of Somalis by Ethiopians as well as deaths, displacement, and orphans resulting from drought and famine occurring at that

time and support by the diaspora of humanitarian relief and the removal of the Ethiopian military from Somali soil.

In assessing sufficiency of the evidence, this Court must determine whether, "after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia,* 307, U.S. 317 (1979). In none of the calls in which Issa Doreh is a participant is there any evidence of his involvement in an agreement to do anything unlawful. There is no agreement as to a conspiracy, to commit murder in Somalia, or to use weapons of mass destruction. There is no evidence at all that Issa Doreh ever knew the name Ayrow, Shikhalow, or al-Shabaab.

In *Jackson v. Virginia,* 443 U.S. at 313-320, this Court held that the Due Process Clause of the 14th Amendment is violated by conviction of a crime without sufficient evidence that each element has been proven beyond a reasonable doubt.[2] It is not enough that Issa Doreh may have known or even associated with the person(s) committing the offenses or unknowingly or unintentionally did things that were helpful to that person or was present at the scene of the crime.

Issa Doreh was the bycatch of bulk collection of metadata, and he did not participate in funding any terrorist. Issa Doreh was a clerk and was unrelated to

[2] *Bolling v. Sharpe*, 347 U.S. 497 (1954), incorporated the 14th Amendment's guarantee of Due Process from the states to apply to the federal government via the Fifth Amendment's Due Process Clause.

any cleric. He is a simple man thrust into a terrorism case because of an illegal spying program. The fact that the evidence against him was insufficient gives the Court ever more reason to grant review and right this wrong.

CONCLUSION

On the basis of the foregoing, the Court should grant the petition for a writ of certiorari.

DATED: July 25, 2025

Respectfully submitted,

/s/ *David Zugman*
Counsel for Mohamed Mohamed Mohamud

/s/ *Elizabeth A. Missakian*
Counsel for Issa Doreh

/s/ *Benjamin Coleman*
Counsel for Ahmed Nasir Taalil Mohamud

APPENDIX

APPENDIX A: Published decision of the Ninth Circuit, filed September 20, 2020

United States v. Moalin

United States Court of Appeals for the Ninth Circuit

February 27, 2025, Filed

No. 13-50572, No. 13-50578, No. 13-50580, No. 14-50051

Reporter
2025 U.S. App. LEXIS 4643 *

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BASAALY SAEED ***MOALIN***, AKA Basal, AKA Muse Shekhnor Roble, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MOHAMED MOHAMED MOHAMUD, AKA Mohamed Khadar, AKA Sheikh Mohamed, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. ISSA DOREH, AKA Sheikh Issa, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. AHMED NASIR TAALIL MOHAMUD, Defendant-Appellant.

Prior History: [*1] D.C. No. 3:10-cr-04246-JM-1, D.C. No. 3:10-cr-04246-JM-2, D.C. No. 3:10-cr-04246-JM-3, D.C. No. 3:10-cr-04246-JM-4. Southern District of California, San Diego.

United States v. ***Moalin***, 973 F.3d 977, 2020 U.S. App. LEXIS 28119, 2020 WL 5225704 (9th Cir. Cal., Sept. 2, 2020)

Counsel: For UNITED STATES OF AMERICA, Plaintiff - Appellee (13-50572, 13-50578, 13-50580, 14-50051): Jeffrey Michael Smith, Washington, DC; Daniel Earl Zipp, Assistant U.S. Attorney, San Diego, CA.

For BASAALY SAEED ***MOALIN***, AKA: Basal, AKA: Muse Shekhnor Roble, Defendant - Appellant (13-50572): Joshua L. Dratel, Law Offices of Joshua L. Dratel, P.C., New York, NY; Alexander A. Abdo, Knight First Amendment Institute at Columbia University, New York, NY; Patrick C. Toomey, American Civil Liberties Union Foundation, Washington, DC.

For BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, AMERICAN LIBRARY ASSOCIATION, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOM TO READ FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, NINTH CIRCUIT FEDERAL AND COMMUNITY DEFENDERS, and REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Amicus Curiae (13-50572, 13-50578, 13-50580, 14-50051): Faiza Patel, Brennan Center for Justice, New York, NY.

For MOHAMED MOHAMED MOHAMUD, AKA: Mohamed Khadar, AKA: Sheikh Mohamed, Defendant - Appellant (13-50578): David **[*2]** James ***Zugman***, Attorney, Burcham & ***Zugman***, San Diego, CA.

For ISSA DOREH, AKA: Sheikh Issa, Defendant - Appellant (13-50580): Elizabeth Armena Missakian, Attorney, Law Office of Elizabeth A. Missakian, San Diego, CA.

For AHMED NASIR TAALIL MOHAMUD, Defendant - Appellant (14-50051): Benjamin Lee Coleman, Benjamin L. Coleman Law, PC, San Diego, CA.

Judges: Before: BERZON and NGUYEN, Circuit Judges, and ZOUHARY,[*] District Judge.

Opinion by: Zouhary

Opinion

The panel has unanimously voted to deny the petitions for rehearing. Judge Nguyen has voted to deny the petitions for rehearing en banc. Judge Berzon and Judge Zouhary recommend denial of the petitions for rehearing en banc. The full court has been advised of the petition for rehearing en banc, and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 40. The petitions for rehearing are denied; the petitions for rehearing en banc are rejected.

Zouhary, J., Statement:

I agree with the decision to deny the petitions for rehearing. I write separately to provide some context on the notice issue.

Section 3504

The government argues 18 U.S.C. § 3504, which allows a defendant to challenge evidence allegedly obtained through unlawful surveillance, provides the proper framework for Appellants **[*3]** to challenge the surveillance evidence in this case. The government points out that "the [P]anel did not cite or address" § 3504. There are two reasons for this. First, a defendant cannot use § 3504 to challenge surveillance if they have no notice of surveillance in the first place. *See, e.g.,* *FBI v. Fazaga*, 595 U.S. 344, 356, 142 S. Ct. 1051, 212 L. Ed. 2d 172 (2022) ("[I]ndividuals affected by FISA surveillance are very often unaware of the surveillance unless it is revealed by the [g]overnment."). But here, Appellants received notice. *United States v.* ***Moalin***, 973 F.3d 977, 998 (9th Cir. 2020) ("After defendants were indicted, the government notified them and the district court that it intended to 'use or disclose' in 'proceedings in this case information obtained or derived from electronic surveillance conducted pursuant to the authority of [FISA].'") (citing 50 U.S.C. § 1806(c)). Second, our Opinion examined whether Appellants were entitled to notice *under the* Fourth Amendment -- not what Appellants *should have done* after receiving that notice (i.e., exercise their rights under § 3504). *See id.* at 999 (discussing notice obligations under *Dalia v. United States*, 441 U.S. 238, 99 S. Ct. 1682, 60 L. Ed. 2d 177 (1979) and 18 U.S.C. § 2518(8)(d)).

National Security

The government also contends that our conclusion on notice will deter cooperation between intelligence agencies and harm national security. There are two problems with this argument. The government assumes our holding **[*4]** requires *disclosure* of sensitive information. As detailed below, the Opinion does no such thing -- *notice* that surveillance took place is all that is required. *See* ***Moalin***, 973 F.3d at 1001 (noting that "notice is distinct from disclosure."). Further, as Appellants point out in their opposition,

[*] The Honorable Jack Zouhary, United States District Judge for the Northern District of Ohio, sitting by designation.

the government has been providing analogous notice under FISA for decades and there is no evidence of a deterrent effect or harm to national security.

Fourth Amendment Notice

Finally, the government challenges our discussion of notice under the Fourth Amendment, arguing this portion of the Opinion is "broad dicta" that runs contrary to congressional intent.

The government asserts that we improperly rely on FISA legislative history that concerned only notice requirements for the execution of search warrants, and that Congress deliberately omitted any notice requirements when the surveillance targets foreigners abroad. As to FISA's legislative history, the government misstates the quoted Senate Report. The Report did not deal with surveillance connected to a warrant. ***Moalin***, 973 F.3d at 1000. But even if the government were correct in its depiction of congressional intent, it makes no difference. This portion of the Opinion, which addressed arguments raised by Appellants, examined **[*5]** what is required by the Fourth Amendment, not FISA. And, more importantly, the Fourth Amendment's applicability is not conditioned on whether there is a warrant or any statutory protection. We state:

> This constitutional notice requirement applies to surveillance conducted under FISA and the [FISA Amendments Act], which codify the requirement. . . . Where statutory protections are lacking, the Fourth Amendment's reasonableness requirement takes on importance as a limit on executive power, and notice is necessary so that criminal defendants may challenge surveillance as inconsistent with that requirement.

Id. at 1000-01.

The government also ignores Appellants' status, arguing the panel "extend[ed] Fourth Amendment rights to cover the government's foreign intelligence activities overseas." At the time of the surveillance, each of the Appellants had either U.S. citizenship or lawful status. ***Moalin***, 973 F.3d at 985 n.2 ("***Moalin*** and Doreh are U.S. citizens, M. Mohamud has refugee status, and Nasir Mohamud has a visa."). Even if the surveillance initially targeted only Al-Shabaab members abroad, the Appellants, all lawfully residing in the U.S., became targets at some point. *See id.* at 999 ("For our purposes, the essential insight of Cavanagh is that even if the Fourth Amendment applies differently in the foreign intelligence **[*6]** context, it still *applies*, at least as U.S. persons are involved.") (citing *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1972)).

The government next argues "[t]he notice rule invented by the [P]anel in this case has no legal basis and has been rejected by at least three other courts." In support, the government cites a single appellate case, *United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021). There, defendant, a lawful permanent resident, received government attention resulting from warrantless § 702 FISA surveillance targeting foreigners abroad. *Id.* at 581. The government used communications obtained through the warrantless surveillance to support further surveillance applications. *Id.* This led to a collection of incriminating statements and the FBI arresting defendant at an airport with cash and other incriminating items. *Id.* But unlike ***Moalin***, the government in that case "filed notice that it had used Section 702 to develop evidence against [him]." *Id.* at 590.

The government asserts that Muhtorov "rejected" a notice requirement. But the opinions don't conflict. Muhtorov concerned, in part, the government's discovery obligations and whether defendant was entitled to *disclosure of* the government's "novel surveillance techniques." 20 F.4th at 632. Our Opinion addressed notice -- not disclosure of techniques -- stating:

> We emphasize that notice is distinct **[*7]** from disclosure. Given the need for secrecy in the foreign intelligence context, the government is required only to inform the defendant that surveillance occurred and that the government intends to use information obtained or derived from it. . . . If the government avers that disclosure of information relating to the surveillance would harm national security, then the court can review the materials bearing on its legality *in camera* and *ex parte*.

Moalin, 973 F.3d at 1001. Additionally, defendant in Muhtorov sought disclosure of surveillance techniques under FISA and the Due Process Clause -- not the Fourth Amendment. 20 F.4th at 630-31.

Though our Fourth Amendment notice ruling may not have been "necessary to decide the case," there are critical reasons for making it. Executive Orders, like EO 12,333, remain outside the scope of FISA and the FAA, and contain no notice requirement. ***Moalin***, 973 F.3d at 999. Again, without any statutory protections, "the Fourth Amendment's reasonableness requirement takes on importance as a limit on executive power, and notice is necessary so that criminal defendants may challenge surveillance as inconsistent with that requirement." *Id.* at 1001. It is for these reasons, the panel struck a balance between the need for secrecy in national-security investigations and a defendant's right to challenge evidence. **[*8]**

End of Document

United States v. Moalin

United States Court of Appeals for the Ninth Circuit

November 10, 2016, Argued and Submitted, Pasadena, California; September 2, 2020, Filed

No. 13-50572, No. 13-50578, No. 13-50580, No. 14-50051x

Reporter
973 F.3d 977 *; 2020 U.S. App. LEXIS 28119 **; 2020 WL 5225704

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BASAALY SAEED ***MOALIN***, AKA Basal, AKA Muse Shekhnor Roble, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MOHAMED MOHAMED MOHAMUD, AKA Mohamed Khadar, AKA Sheikh Mohamed, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. ISSA DOREH, AKA Sheikh Issa, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. AHMED NASIR TAALIL MOHAMUD, Defendant-Appellant.

Prior History: **[**1]** Appeal from the United States District Court for the Southern District of California. D.C. No. 3:10-cr-04246-JM-1, D.C. No. 3:10-cr-04246-JM-2, D.C. No. 3:10-cr-04246-JM-3, D.C. No. 3:10-cr-04246-JM-4. Jeffrey T. Miller, District Judge, Presiding.

*United States v. **Moalin**, 2013 U.S. Dist. LEXIS 164038 (S.D. Cal., Nov. 18, 2013)*

Syllabus

SUMMARY[**]

Criminal Law

The panel affirmed the convictions of four members of the Somali diaspora for sending, or conspiring to send, $10,900 to Somalia to support a foreign terrorist organization, in an appeal that raised complex questions regarding the U.S. government's authority to collect bulk data about its citizens' activities under the auspices of a foreign intelligence investigation, as well as the rights of criminal defendants when the prosecution uses information derived from foreign intelligence surveillance.

The panel held that the government may have violated the *Fourth Amendment* when it collected the telephony metadata of millions of Americans, including at least one of the defendants, pursuant to the *Foreign Intelligence Surveillance Act* (FISA), but that suppression is not warranted on the facts of this case. Having carefully reviewed the classified FISA applications and all related classified information, the panel was convinced that under established **[**2]** *Fourth Amendment* standards, the metadata collection, even if unconstitutional, did not taint the evidence introduced by the government at trial. The panel wrote that to the extent the public

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

statements of government officials created a contrary impression, that impression is inconsistent with the contents of the classified record.

The panel rejected the government's argument that the defendants lacked standing to pursue their statutory challenge to the (subsequently discontinued) metadata collection program. On the merits, the panel held that the metadata collection exceeded the scope of Congress's authorization in *50 U.S.C. § 1861*, which required the government to make a showing of relevance to a particular authorized investigation before collecting the records, and that the program therefore violated that section of FISA. The panel held that suppression is not clearly contemplated by *section 1861*, and there is no statutory basis for suppressing the metadata itself. The panel's review of the classified record confirmed that the metadata did not and was not necessary to support the requisite probable cause showing for the FISA Subchapter I warrant application in this case. The panel wrote that even if it were to apply a "fruit **[**3]** of the poisonous tree" analysis, it would conclude that evidence from the government's wiretap of defendant ***Moalin***'s phone was not the fruit of the unlawful metadata collection. The panel wrote that if the statements of the public officials created a contrary impression, that impression is inconsistent with the facts presented in the classified record.

The panel confirmed that the *Fourth Amendment* requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from the surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities. The panel did not decide whether the government failed to prove any required notice in this case because the lack of such notice did not prejudice the defendants.

The panel held that evidentiary rulings challenged by the defendants did not, individually or cumulatively, impermissibly prejudice the defense.

The panel held that sufficient evidence supported defendant Doreh's convictions.

Counsel: Joshua L. Dratel (argued), Joshua Dratel P.C., New York, New York; Alexander A. Abdo (argued), Jameel Jaffer, Patrick Toomey, and Brett Max Kaufman, American Civil **[**4]** Liberties Union, New York, New York; David J. Zugman, Burcham & Zugman, San Diego, California; Elizabeth Armena Missakian, Law Office of Elizabeth A. Missakian, San Diego, California; Benjamin L. Coleman, Coleman & Balogh LLP, San Diego, California; for Defendants-Appellants.

Jeffrey M. Smith (argued), Appellate Counsel; John P. Carlin, Assistant Attorney General; National Security Division, United States Department of Justice, Washington, D.C.; Caroline P. Han, Assistant United States Attorney; United States Attorney's Office, San Diego, California; for Plaintiff-Appellee.

Michael Price, Brennan Center for Justice, New York, New York; Faiza Patel, Brennan Center for Justice at New York University School of Law, New York, New York; Alan Butler, Electronic Privacy Information Center (EPIC), Washington, D.C.; David M. Porter, Co-Chair, NACDL Amicus Committee; Sacramento, California; Bruce D. Brown, Katie Townsend, and Hannah Bloch-Wehba, Reporters Committee for Freedom of the Press, Washington, D.C.; Michael Filipovic, Federal Public Defender, Seattle, Washington; Tony Gallagher, Executive Director,

Federal Defenders of Montana, Great Falls, Montana; Lisa Hay, Federal Public Defender, **[**5]** Portland, Oregon; Heather Erica Williams, Federal Public Defender, Sacramento, California; Steven Gary Kalar, Federal Public Defender, San Francisco, California; Hilary Potashner, Federal Public Defender, Los Angeles, California; Reuben Cahn, Executive Director, Federal Defenders of San Diego Inc., San Diego, California; Jon M. Sands, Federal Public Defender, Phoenix, Arizona; Rich Curtner, Federal Public Defender, Anchorage, Alaska; John T. Gorman, Federal Public Defender, Mong Mong, Guam; Peter Wolff, Federal Public Defender, Honolulu, Hawaii; Samuel Richard Rubin, District of Idaho Community Defender, Boise, Idaho; R.L. Valladares, Federal Public Defender, Las Vegas, Nevada; for Amici Curiae Brennan Center for Justice, American Library Association, Electronic Privacy Information Center, Freedom to Read Foundation, National Association of Criminal Defense Lawyers, Ninth Circuit Federal and Community Defenders, and Reporters Committee for Freedom of the Press.

Judges: Before: Marsha S. Berzon and Jacqueline H. Nguyen, Circuit Judges, and Jack Zouhary,[*] District Judge. Opinion by Judge Berzon.

Opinion by: Marsha S. Berzon

Opinion

[*984] BERZON, Circuit Judge:

INTRODUCTION

Four members of the Somali diaspora appeal from their **[**6]** convictions for sending, or conspiring to send, $10,900 to Somalia to support a foreign terrorist organization. Their appeal raises complex questions regarding the U.S. government's authority to collect bulk data about its citizens' activities under the auspices of a foreign intelligence investigation, as well as the rights of criminal defendants when the prosecution uses information derived from foreign intelligence surveillance. We conclude that the government may have violated the *Fourth Amendment* and did violate the *Foreign Intelligence Surveillance Act ("FISA")* when it collected the telephony metadata of millions of Americans, including at least one of the defendants, but suppression is not warranted on the facts of this case. Additionally, we confirm that the *Fourth Amendment* requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities. We do not decide whether the government failed to provide any required notice in this case because the lack of such notice did not prejudice the defendants. After considering **[*985]** these **[**7]** issues and several others raised by the defendants, we affirm the convictions in all respects.

BACKGROUND[1]

[*] The Honorable Jack Zouhary, United States District Judge for the Northern District of Ohio, sitting by designation.

I.

Somalia's turbulent recent history forms the backdrop for this case. After military dictator Siad Barre was ousted in 1991, the country spiraled into civil war. Fighting between rival warlords led to a humanitarian crisis in Mogadishu, Somalia's capital, and other parts of the country. An estimated 30,000 people died in Mogadishu alone, and hundreds of thousands more were displaced. As the war continued, its impact on the populace was exacerbated by recurring periods of severe drought and famine.

In 2004, an interim government for Somalia, the Transitional Federal Government ("TFG"), was established in Kenya. Although the TFG received significant international support, it faced widespread distrust and opposition in Somalia. The TFG installed itself in Somalia with the protection of Ethiopian military forces, which occupied Somalia beginning in 2006. Somali opposition to the TFG and the Ethiopian occupation developed into a broad-based, violent insurgency undertaken by a variety of groups with disparate agendas.

One element of the insurgency was a group called "al-Shabaab," which **[**8]** means "the youth" in Arabic. Al-Shabaab used distinctive types of violence, such as improvised explosive devices and suicide bombings. In March 2008, the United States designated al-Shabaab a foreign terrorist organization. A key figure in al-Shabaab, Aden Hashi Ayrow, was killed in a U.S. missile strike on May 1, 2008.

Many Somalis have fled the country. An estimated three million live abroad, creating a global Somali diaspora. Somalis abroad often remain actively engaged in developments in Somalia, and contributions from the diaspora are a critical source of financial support within the troubled country. As Somalia has no formal banking system, members of the diaspora who wish to send money back frequently rely on informal money transfer businesses called "hawalas."

II.

Defendants Basaaly Saeed ***Moalin*** ("***Moalin***"), Mohamed Mohamed Mohamud ("M. Mohamud"), Issa Doreh ("Doreh"), and Ahmed Nasir Taalil Mohamud ("Nasir Mohamud") immigrated to the United States from Somalia years ago and lived in Southern California.[2] ***Moalin*** and Nasir Mohamud were taxicab drivers; M. Mohamud was an imam at a mosque; and Doreh worked at Shidaal Express, a hawala.

Between October 2010 and June 2012, the United **[**9]** States ("the government") charged defendants in a five-count indictment with conspiring to send and sending $15,900 to Somalia between January and August of 2008 to support al-Shabaab.[3] The charges against all four defendants were: conspiracy to provide material support to terrorists, in violation of *18 U.S.C. § 2339A(a)*; conspiracy to provide material support to a foreign terrorist organization, in violation of

---

[1] All the factual information presented in this opinion comes from unclassified or declassified sources.

[2] ***Moalin*** and Doreh are U.S. citizens, M. Mohamud has refugee status, and Nasir Mohamud has a visa.

[3] At trial, the government sought only to prove that defendants had sent $10,900 to support al-Shabaab.

18 U.S.C. § 2339B(a)(1); and conspiracy to launder monetary instruments, **[*986]** in violation of 18 U.S.C. § 1956(a)(2)(A) and (h). ***Moalin***, M. Mohamud, and Doreh were charged with an additional count of providing material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B(a)(1) and (2), and ***Moalin*** was charged with a further count of conspiracy to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a), based on his alleged provision of a house in Somalia to members of al-Shabaab.

Shortly after filing the initial indictment, the government filed notice that it intended to use or disclose in the proceedings "information obtained or derived from electronic surveillance conducted pursuant to the authority of the Foreign Intelligence Surveillance Act." At trial, the government's principal evidence against defendants consisted of a series of recorded calls **[**10]** between ***Moalin***, his codefendants, and individuals in Somalia, obtained through a wiretap of ***Moalin***'s phone. The government obtained access to ***Moalin***'s calls after receiving a court order under FISA Subchapter I, 50 U.S.C. §§ 1801-1812. Several of the recorded calls involved a man who went by "Shikhalow" (sometimes spelled "Sheikalow") or "Majadhub," whom the government contends was Ayrow, the important al-Shabaab figure. In addition to the intercepted phone calls, the government introduced records of money transfers completed by Shidaal Express, the hawala where Doreh worked.

In a recorded call from December 2007, Shikhalow requested money from ***Moalin*** for "rations." The two men also discussed other fundraising efforts relating to a school. ***Moalin*** then spoke with Doreh, reporting that "[o]ne dollar a day per man" was needed for forces stationed "where the fighting [is] going on." ***Moalin*** also spoke with Nasir Mohamud, telling him that money was needed for "the young men who are firing the bullets" and that, within the last month, "these men cut the throats of 60" Ethiopians and destroyed up to five vehicles.

Ten days later, ***Moalin*** called Shikhalow to tell him that he had sent $3,300 using the recipient name **[**11]** "Yusuf Mohamed Ali." Transaction records from the Shidaal Express reveal two transfers of $1,950 each to "yusuf mohamed ali" from "Duunkaal warsame warfaa" and "safiya Hersi." Two days later, ***Moalin*** called Shikhalow again, and Shikhalow told him he had "received the three." ***Moalin*** also offered Shikhalow the use of one of his houses in Somalia, which, ***Moalin*** noted, had an attic suitable for hiding documents and weapons. A half-hour after making the call to Shikhalow, ***Moalin*** told another acquaintance he "was talking to the man who is in charge of the youth."

Later, in January 2008, ***Moalin*** called Shikhalow again, urging him to allow another group to handle "overall politics" while Shikhalow dealt with "military matters." Shikhalow disagreed, stating, "we, the Shabaab, have a political section, a military section and a missionary section." Shikhalow recounted recent incidents in which his group had planted a landmine and launched mortar shells at the presidential palace, and requested more money "to support the insurgent."

Communications between ***Moalin*** and Shikhalow continued through April 2008, during which time several money transfers were made to "yusuf mohamed ali," "YUSUF MOHAMED ALI," **[**12]** "DUNKAAL MOHAMED YUSUF," and "mohamed yusuf dunkaal." Ayrow was killed on May 1, 2008. A week later, ***Moalin*** told an acquaintance that he did not want "the assistance and the work that we were performing" to stop, even though "the man that we used to deal with is gone."

In July 2008, a senior operational figure in al-Shabaab gave ***Moalin*** contact information **[*987]** for Omar Mataan. Later that day, ***Moalin*** got in touch with Mataan and promised to send money. The following week, ***Moalin*** spoke with Nasir Mohamud, reporting that they were being "closely watched," but that they could still support "the orphans" and "people in need" and would "go under that pretense now." Shidaal Express records show a series of transfers over the next few weeks, including one to "Omer Mataan" and another to "Omer matan."[4]

Defendants did not dispute that they sent money to Somalia through Shidaal Express, but they did dispute that the money was intended to support al-Shabaab. They maintained that Shikhalow was not Ayrow but a local police commissioner, and that their money went to support the work of regional administrations governing in the absence of an effective central government. ***Moalin*** also presented evidence that **[**13]** he supported humanitarian causes in Somalia during the time period of the indictment.

In February 2013, the jury convicted defendants on all counts.

III.

Before trial, ***Moalin*** moved to suppress, among other things, "all interceptions made and electronic surveillance conducted pursuant to [FISA], *50 U.S.C. § 1801, et seq.*, and any fruits thereof, and/or for disclosure of the underlying applications for FISA warrants." ***Moalin*** contended that information in the government's applications for the FISA wiretap may have been "generated by illegal means"—that is, that the government may have violated the *Fourth Amendment* or its statutory authority under FISA in collecting information supporting the FISA warrants. The district court denied ***Moalin***'s suppression motion and did not grant security-cleared defense counsel access to the documents supporting the FISA orders.

Two days before trial, the prosecution disclosed an email from a redacted FBI email address to the government's Somali linguist, who was monitoring ***Moalin***'s phone calls during the wiretap. The email said: "We just heard from another agency that Ayrow tried to make a call to Basaaly [***Moalin***] today, but the call didn't go through. If you see anything today, can you give us a **[**14]** shout? We're extremely interested in getting real-time info (location/new #'s) on Ayrow."

Months after the trial, in June 2013, former National Security Agency ("NSA") contractor Edward Snowden made public the existence of NSA data collection programs. One such program, conducted under FISA Subchapter IV, involved the bulk collection of phone records, known as telephony metadata, from telecommunications providers. Other programs, conducted under the *FISA Amendments Act of 2008*, involved the collection of electronic communications, such as email messages and video chats, including those of people in the United States.

Subsequent statements of public officials defending the telephony metadata collection program averred that the program had played a role in the government's investigation of ***Moalin***. These statements reported that the FBI had previously closed an investigation focused on ***Moalin***

[4] We review the call transcripts in greater deal in Part V of the Discussion section of the opinion, *infra* pp. 53-57.

without bringing charges, then reopened that investigation based on information obtained from the metadata program.

For instance, in a hearing before the House Permanent Select Committee on Intelligence held shortly after the Snowden **[*988]** disclosures, then-FBI Deputy Director Sean Joyce described a post-9/11 **[**15]** investigation conducted by the FBI that initially "did not find any connection to terrorist activity. Several years later, under [FISA Subchapter IV], the NSA provided us a telephone number only in San Diego that had indirect contact with an extremist outside the United States." Joyce explained that the FBI "served legal process to identify who was the subscriber to this telephone number," then, after "further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA Court, we were able to identify co-conspirators, and we were able to disrupt" their financial support to a Somali designated terrorist group. According to Joyce, "if [the FBI] did not have the tip from NSA, [it] would not have been able to reopen that investigation." In another congressional hearing, Joyce specifically named ***Moalin*** as the target of the investigation.

On September 30, 2013, defendants filed a motion for a new trial. Defendants argued that the government's collection and use of ***Moalin***'s telephony metadata violated the *Fourth Amendment*, and that the government had failed to provide notice of the metadata collection or of any surveillance of ***Moalin*** it had conducted under the **[**16]** FISA Amendments Act, including, potentially, the surveillance referred to in the email to the linguist. The district court denied the motion, concluding that "public disclosure of the NSA program adds no new facts to alter the court's FISA . . . rulings," and that the telephony metadata program did not violate the *Fourth Amendment*. *United States v. **Moalin**, No. 10-CR-4246 JM, 2013 U.S. Dist. LEXIS 164038, 2013 WL 6079518, at *4, *8 (S.D. Cal. Nov. 18, 2013)*.

This appeal followed. On appeal, defendants continue to challenge the metadata collection and the lack of notice of both the metadata collection and of any additional surveillance not disclosed by the government. They also make arguments regarding the government's obligation to produce exculpatory evidence; the district court's evidentiary rulings; and the sufficiency of the evidence to convict Doreh. We present the facts relating to each argument as we analyze it.

DISCUSSION

I. The Telephony Metadata Collection Program

The government's telephony metadata collection program was authorized in a series of classified orders by the FISA Court under FISA Subchapter IV, the "business records" subchapter.[5] *See* *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*

[5] The FISA Court was established by Congress to entertain applications by the government to take investigative actions authorized by FISA. ***50 U.S.C. § 1803(a)***. Broadly, "FISA authorizes the federal government to engage in four types of investigative activity [in the United States]: electronic surveillance targeting foreign powers and agents of foreign powers; physical searches targeting foreign powers and agents of foreign powers; the use of pen registers and trap-and-trace devices . . . ; and court orders compelling the production of tangible things in connection with certain national security investigations." David Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 4:2 (3rd ed. 2019).

from [redacted], No. BR 13-80, 2013 U.S. Dist. LEXIS 147002, 2013 WL 5460137, at *1 (FISA Ct. Apr. 25, 2013). These orders required major **[**17]** telecommunications providers to turn over to the government on an "ongoing daily" basis a "very large volume" of their "call detail records." In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [redacted], No. BR 13-109, 2013 U.S. Dist. LEXIS 134786, 2013 WL 5741573, at *1 (FISA Ct. Aug. 29, 2013) **[*989]** ("In re Application II"). Specifically, providers were ordered to produce "all call detail records or 'telephony metadata' . . . for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." 2013 U.S. Dist. LEXIS 134786, [WL] at *10. These records included information such as the phone numbers involved in a call and the time and duration of the call, but not the voice content of any call. 2013 U.S. Dist. LEXIS 134786, [WL] at *1 n.2.

The court orders authorized the NSA to compile the records into a database and to query the database under certain conditions to obtain foreign intelligence information. *See* 2013 U.S. Dist. LEXIS 134786, [WL] at *1. During the time period relevant to this case, the government was permitted to search the database when certain NSA officials determined that "reasonable, articulable suspicion" existed connecting a specific selection term—for example, a particular phone number—with "one of the identified international **[**18]** terrorist organizations." *Id.* The government was also allowed to search phone numbers within three "hops" of that selector, *i.e.*, the phone numbers directly in contact with a selector, the numbers that had been in contact with those numbers, and the numbers that had been in contact with those numbers. In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [redacted], No. BR 14-96, 2014 U.S. Dist. LEXIS 157864, 2014 WL 5463290, at *2 & n.2 (FISA Ct. June 19, 2014).

Snowden's disclosure of the metadata program prompted significant public debate over the appropriate scope of government surveillance. In June 2015, Congress passed the *USA FREEDOM Act*, which effectively ended the NSA's bulk telephony metadata collection program. *Pub. L. No. 114-23, 129 Stat. 268* (codified at 50 U.S.C. § 1861). The Act prohibited further bulk collection of phone records after November 28, 2015. *Id.*; *see* Smith v. Obama, 816 F.3d 1239, 1241 (9th Cir. 2016). Besides ending the bulk collection program, Congress also established new reporting requirements relating to the government's collection of call detail records. *Pub. L. No. 114-23, § 601, 129 Stat. at 291*.

Defendants contend that the discontinued metadata program violated both the Fourth Amendment and FISA Subchapter IV, under which it was authorized. They argue that the "fruits" of the government's acquisition of ***Moalin***'s phone records **[**19]** should therefore have been suppressed. According to defendants, those fruits included the phone records themselves and the evidence the government obtained through its subsequent wiretap of ***Moalin***'s phone.

A.

Moalin contends that the metadata collection violated his Fourth Amendment "right . . . to be secure . . . against unreasonable searches and seizures." U.S. Const. amend. IV. A person may invoke the protections of the Fourth Amendment by showing he had "an actual (subjective) expectation of privacy," and "the expectation [is] one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)

(Harlan, J., concurring). ***Moalin*** asserts he had a reasonable expectation of privacy in his telephony metadata.

The district court held, and the government argues, that this case is controlled by *Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)*, which helped establish the so-called third-party doctrine in *Fourth Amendment* jurisprudence. *Smith* held that the government's use of a pen register to record the numbers the defendant dialed from his home telephone did not constitute a *Fourth Amendment* search, because individuals have no reasonable expectation of privacy in information **[*990]** they voluntarily convey to the telephone company. *Id. at 742-43*. *Smith* relied on *United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976)*, which had held that defendants had no legitimate expectation of privacy in their bank **[**20]** records. The government argues that the NSA's collection of ***Moalin***'s telephony metadata is indistinguishable, for *Fourth Amendment* purposes, from the use of the pen register in *Smith*.

There are strong reasons to doubt that *Smith* applies here. Advances in technology since 1979 have enabled the government to collect and analyze information about its citizens on an unprecedented scale. Confronting these changes, and recognizing that a "central aim" of the *Fourth Amendment* was "to place obstacles in the way of a too permeating police surveillance," the Supreme Court recently declined to "extend" the third-party doctrine to information whose collection was enabled by new technology. *Carpenter v. United States, 138 S. Ct. 2206, 2214, 2217, 201 L. Ed. 2d 507 (2018)* (quoting *United States v. Di Re, 332 U.S. 581, 595, 68 S. Ct. 222, 92 L. Ed. 210 (1948))*.

Carpenter did not apply the third-party doctrine to the government's acquisition of historical cell phone records from the petitioner's wireless carriers. The records revealed the geographic areas in which the petitioner used his cell phone over a period of time. *Id. at 2220*. Citing the "unique nature of cell phone location information," the Court concluded in *Carpenter* that "the fact that the Government obtained the information from a third party does not overcome [the petitioner's] claim to *Fourth Amendment* protection," because there is "a world of difference **[**21]** between the limited types of personal information addressed in *Smith* . . . and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id. at 2219-20*.

There is a similar gulf between the facts of *Smith* and the NSA's long-term collection of telephony metadata from ***Moalin*** and millions of other Americans. In *Smith*, a woman was robbed and gave the police a description of the robber and of a car she saw nearby. *442 U.S. at 737*. After the robbery, the woman received "threatening and obscene phone calls from a man identifying himself as the robber." *Id.* Police later spotted a man and car matching the robber's description and traced the license plate number to Smith. *Id.* Without obtaining a warrant, they asked the telephone company to install a "pen register," a device that would record the numbers dialed from Smith's home telephone. *Id.* The day the pen register was installed it recorded a call from Smith's home to the home of the robbery victim. *Id.* Based on that and other evidence, police obtained a warrant to search Smith's home and arrested him two days later. *Id.*

Holding that the use of the pen register did not constitute a "search" for *Fourth Amendment* purposes, *id. at 745-46*, the Court reasoned, first, **[**22]** that it was unlikely "that people in general entertain any actual expectation of privacy in the numbers they dial," *id. at 742*. Second, "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would

remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'" *Id. at 743* (quoting *Katz, 389 U.S. at 361*). Smith had "voluntarily conveyed numerical information to the telephone company" and in so doing had "assumed the risk that the company would reveal to police the numbers he dialed." *Id. at 744*.

The distinctions between *Smith* and this case are legion and most probably constitutionally significant. To begin with, the **[*991]** type of information recorded in *Smith* was "limited" and of a less "revealing nature" than the telephony metadata at issue here. *Carpenter, 138 S. Ct. at 2219*. The pen register did not disclose the "identities" of the caller or of the recipient of a call, "nor whether the call was even completed." *Smith, 442 U.S. at 741* (quoting *United States v. New York Tel. Co., 434 U.S. 159, 167, 98 S. Ct. 364, 54 L. Ed. 2d 376 (1977)*). In contrast, the metadata in this case included "comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International **[**23]** Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." *In re Application II, 2013 U.S. Dist. LEXIS 134786, 2013 WL 5741573, at *1 n.2*. "IMSI and IMEI numbers are unique numbers associated with a particular telephone user or communications device." Br. of Amici Curiae Brennan Center for Justice 11. "A 'trunk identifier' provides information about where a phone connected to the network, revealing data that can locate the parties within approximately a square kilometer." *Id.* at 11-12.

Although the *Smith* Court perceived a significant distinction between the "contents" of a conversation and the phone number dialed, *see 442 U.S. at 743*, in recent years the distinction between content and metadata "has become increasingly untenable," as Amici point out. Br. of Amici Curiae Brennan Center for Justice 6. The amount of metadata created and collected has increased exponentially, along with the government's ability to analyze it. "Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life." *Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013)*, *vacated and remanded*, *800 F.3d 559, 419 U.S. App. D.C. 199 (D.C. Cir. 2015)*. According to the NSA's former general counsel Stewart Baker, "[m]etadata absolutely tells **[**24]** you everything about somebody's life. . . . If you have enough metadata you don't really need content . . . ." Laura K. Donohue, *The Future of Foreign Intelligence* 39 (2016). The information collected here was thus substantially more revealing than the telephone numbers recorded in *Smith*.

The duration of the collection in this case—and so the amount of information collected—also vastly exceeds that in *Smith*. While the pen register in *Smith* was used for a few days at most, here the NSA collected ***Moalin***'s (and millions of other Americans') telephony metadata on an ongoing, daily basis for years. *Carpenter* distinguished between using a beeper to track a car "during a discrete automotive journey," which the Court had upheld in *United States v. Knotts, 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983)*, and using cell phone location information to reveal "an all-encompassing record of the holder's whereabouts" "over the course of 127 days." *138 S. Ct. at 2215, 2217* (internal quotation marks omitted). As the Court put it, "Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible." *Id. at 2219*.

Like the cell phone location information in *Carpenter*, telephony metadata, **[**25]** "as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls . . . permit something akin to . . . 24-hour surveillance . . . ." *Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015)*. This long-term surveillance, made possible by new technology, upends **[*992]** conventional expectations of privacy. Historically, "surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." *United States v. Jones, 565 U.S. 400, 429, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012)* (Alito, J., concurring in the judgment). Society may not have recognized as reasonable Smith's expectation of privacy in a few days' worth of dialed numbers but is much more likely to perceive as private several years' worth of telephony metadata collected on an ongoing, daily basis—as demonstrated by the public outcry following the revelation of the metadata collection program.

Also problematic is the extremely large number of people from whom the NSA collected telephony metadata, enabling the data to be aggregated and analyzed in bulk. The government asserts that "the fact that the NSA program also involved call records relating to other people . . . is irrelevant because *Fourth Amendment* rights . . . cannot be raised vicariously." **[**26]** Br. of United States 58. The government quotes the FISA Court, which reasoned similarly that "where one individual does not have a *Fourth Amendment* interest, grouping together a large number of similarly-situated individuals cannot result in a *Fourth Amendment* interest springing into existence *ex nihilo*." *In re Application II, 2013 U.S. Dist. LEXIS 134786, 2013 WL 5741573, at *2*. But these observations fail to recognize that the collection of millions of other people's telephony metadata, and the ability to aggregate and analyze it, makes the collection of ***Moalin***'s *own* metadata considerably more revealing.

A couple of examples illustrate this point: A woman calls her sister at 2:00 a.m. and talks for an hour. The record of that call reveals some of the woman's personal information, but more is revealed by access to the sister's call records, which show that the sister called the woman's husband immediately afterward. Or, a police officer calls his college roommate for the first time in years. Afterward, the roommate calls a suicide hotline. These are simple examples; in fact, metadata can be combined and analyzed to reveal far more sophisticated information than one or two individuals' phone records convey. As Amici explain, "it is relatively simple to superimpose our metadata trails onto **[**27]** the trails of everyone within our social group and those of everyone within our contacts' social groups and quickly paint a picture that can be startlingly detailed"—for example, "identify[ing] the strength of relationships and the structure of organizations." Br. of Amici Curiae Brennan Center for Justice 21 (internal quotation marks and alterations omitted). Thus, the very large number of people from whom telephony metadata was collected distinguishes this case meaningfully from *Smith*.

Finally, numerous commentators and two Supreme Court Justices have questioned the continuing viability of the third-party doctrine under current societal realities. The assumption-of-risk rationale underlying the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones, 565 U.S. at 417* (Sotomayor, J., concurring). "Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* . . . teach[es] that the police can review all of this material,

on the theory that no one reasonably expects any of it will be kept **[**28]** private. But no one believes that, if they ever did." *Carpenter, 138 S. Ct. at 2262* (Gorsuch, J., dissenting).

For all these reasons, defendants' *Fourth Amendment* argument has considerable force. But we do not come to rest as to whether the discontinued metadata program **[*993]** violated the *Fourth Amendment* because even if it did, suppression would not be warranted on the facts of this case. *See United States v. Ankeny, 502 F.3d 829, 836-37 (9th Cir. 2007)* (declining to decide "close" *Fourth Amendment* question where suppression was "not appropriate"). Having carefully reviewed the classified FISA applications and all related classified information, we are convinced that under established *Fourth Amendment* standards, the metadata collection, even if unconstitutional, did not taint the evidence introduced by the government at trial. *See Wong Sun v. United States, 371 U.S. 471, 488, 83 S. Ct. 407, 9 L. Ed. 2d 441 (1963)*. To the extent the public statements of government officials created a contrary impression, that impression is inconsistent with the contents of the classified record.[6]

B.

Defendants also argue that the metadata collection program violated FISA Subchapter IV, under which the FISA Court authorized it.

1.

At the outset, the government asserts that ***Moalin*** lacks standing to pursue his statutory challenge. The government relies on *United States v. Plunk, 153 F.3d 1011 (9th Cir. 1998)*, *overruled on other grounds by United States v. Hankey, 203 F.3d 1160, 1169 n.7 (9th Cir. 2000)*. *Plunk* held **[**29]** that a defendant lacked *Fourth Amendment* "standing" to challenge a subpoena to his telephone company requesting his telephone records. *Id. at 1020*. We reasoned in *Plunk* that the subpoena was directed not at the defendant "but rather at third party businesses," and that "individuals possess no reasonable expectation of privacy in telephone records." *Id.* [7] The government challenges ***Moalin***'s standing on the same basis, which it

---

[6] Defendants, relying on *Alderman v. United States, 394 U.S. 165, 89 S. Ct. 961, 22 L. Ed. 2d 176 (1969)*, urge us to remand to the district court for a suppression hearing. *Alderman* held that where the government conducted electronic surveillance of defendants in violation of the *Fourth Amendment*, the government had to turn over to defendants "the records of those overheard conversations" so that they could intelligently litigate the question whether the unlawful eavesdropping had tainted the evidence introduced at trial. *Id. at 183*. The Court in *Alderman* was concerned that if it were left solely to the trial judge to review the recorded conversations *in camera*, the judge might lack the time or knowledge to grasp the significance of an "apparently innocent phrase" or "chance remark" that in fact shaped the subsequent investigation. *Id. at 182-84*.

We decline to extend *Alderman*'s holding to the facts of this case. Here, the material whose collection may have been unlawful but was not disclosed was not ***Moalin***'s conversations but his telephony metadata; the records of the overheard conversations obtained pursuant to the FISA warrants were fully disclosed. We express no opinion as to whether *Alderman* could appropriately apply to the government's unlawful collection of metadata in a different case. But in the particular circumstances of this case, based on our careful review of the classified record, there is no concern similar to the Court's concern in *Alderman* and thus no need to apply the case here, given the countervailing national security concerns.

[7] *Plunk* also concluded that the defendant had "not demonstrated that he was within the 'zone of interests' intended to be protected by" the statutory provision at issue in that case, *id.*, but the government does not raise a similar argument here.

contends "is simply an application of the broader rule that 'the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant.'" Br. of United States 51 (quoting *Miller, 425 U.S. at 444*).

As our cases have explained, "*Fourth amendment* standing is quite different . . . **[*994]** from 'case or controversy' determinations of article III standing." *United States v. Taketa, 923 F.2d 665, 669 (9th Cir. 1991)*. Whereas Article III standing concerns our jurisdiction, *Fourth Amendment* standing "is a matter of substantive *fourth amendment* law; to say that a party lacks *fourth amendment* standing is to say that *his* reasonable expectation of privacy has not been infringed." *Id.*[8]

We reject the government's invitation to dispense with defendants' statutory argument on the basis of *Fourth Amendment* standing. First, as *Carpenter* clarified after this case was briefed, there is no categorical rule preventing criminal **[**30]** defendants from challenging third-party subpoenas. *Carpenter, 138 S. Ct. at 2221*. Second, as discussed above, ***Moalin*** likely had a reasonable expectation of privacy in his telephony metadata—at the very least, it is a close question. Finally, and most importantly, defendants' statutory and *Fourth Amendment* arguments rest on independent legal grounds, and we see no reason why ***Moalin***'s "standing" to pursue the statutory challenge should turn on the merits of the *Fourth Amendment* issue. We therefore proceed to the merits of the statutory challenge.

2.

Section 1861 of FISA Subchapter IV authorizes the government to apply to the FISA Court for an "order requiring the production of any tangible things (including . . . records . . .) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *50 U.S.C. § 1861(a)(1)*.[9] At the time relevant to this case, the statute required the government to include in its application "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant to an authorized investigation* (other than a threat assessment)." *50 U.S.C. § 1861(b)(2)(A) (2006)* (emphasis added).[10] Defendants argue that the metadata **[**31]** program defied this relevance requirement because the government collected phone records in bulk, without regard to whether any individual record was relevant to any specific, already-authorized investigation.

The government's theory, expressed in its initial application to the FISA Court to authorize the metadata collection, was that "[a]lthough admittedly a substantial portion of the telephony metadata that is collected would not relate to operatives of [redacted], the intelligence tool that the Government hopes to use to find [redacted] communications—metadata analysis—requires collecting and storing large volumes of the metadata to enable later analysis." Mem. of Law in

---

[8] Unlike *Clapper v. Amnesty Int'l USA, 568 U.S. 398, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013)*, this case is a criminal prosecution, so there is no Article III standing issue here.

[9] All citations to the U.S. Code are to the current version unless otherwise indicated.

[10] The USA Freedom Act later expanded on the application requirements. *See 50 U.S.C. § 1861(b)(2)(A)-(C)*.

Supp. of Appl. for Certain Tangible Things for Investigations to Protect Against International Terrorism 15, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 06-05, 2006 U.S. Dist. LEXIS 101368 (FISA Ct. May 23, 2006)*. According to the government, "[a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection." *Id.*

Defendants respond that Congress intended for the relevance requirement to be a limiting principle. They argue that the government's **[**32]** interpretation of the word **[*995]** "relevant" is essentially limitless and so contravenes the statute. Defendants rely principally on *Clapper*, which held that the text of *section 1861* "cannot bear the weight the government asks us to assign to it, and . . . does not authorize the telephone metadata program." *785 F.3d at 821*. We agree.

As the Second Circuit noted, the "expansive concept of 'relevance'" used by the government to justify the metadata program "is unprecedented and unwarranted." *Id. at 812*. The government had argued in *Clapper* that Congress's intention in adopting *section 1861* was to give the government "broad-ranging investigative powers analogous to those traditionally used in connection with grand jury investigations into possible criminal behavior." *Id. at 811*. Although the Second Circuit agreed with that premise, it concluded that the metadata collection orders were dissimilar from grand jury subpoenas with respect to both the quantity and the quality of the information sought. First, "while . . . subpoenas for business records may encompass large volumes of paper documents or electronic data, the most expansive of such evidentiary demands are dwarfed by the volume of records obtained pursuant to the orders in question here." *Id. at 813*. Second, **[**33]** "document subpoenas typically seek the records of a particular individual or corporation under investigation, and cover particular time periods when the events under investigation occurred," but the metadata collection orders "contain[ed] no such limits." *Id.*

The Second Circuit also reasoned that the term "relevant" in *section 1861* takes meaning from its context: records sought must be "relevant to an *authorized* investigation." *50 U.S.C. § 1861(b)(2)(A) (2006)* (emphasis added). The court faulted the government for referring to the records collected under the metadata program "as relevant to 'counterterrorism investigations,' without identifying any specific investigations to which such bulk collection is relevant." *Clapper, 785 F.3d at 815*.

Here, the government, in the two pages it devotes to defending the metadata program's compliance with FISA, maintains that the Second Circuit got it wrong because "[t]here were in fact multiple specified counterterrorism investigations for which the [FISA Court], in repeatedly approving the program, found reasonable grounds to believe the telephony metadata would be relevant." Br. of United States 53. But, as the Second Circuit noted, referring to the findings of the Privacy and Civil Liberties Oversight **[**34]** Board ("PCLOB") in a 2014 report on the metadata collection program:

> [T]he government's practice is to list in *§ [1861]* applications multiple terrorist organizations, and to declare that the records being sought are relevant to the investigations of all of those groups. . . . As the [PCLOB] report puts it, that practice is "little different, in practical terms, from simply declaring that they are relevant to counterterrorism in general. . . . At its core,

> the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations."

785 F.3d at 815 (quoting Privacy and Civil Liberties Oversight Board, Rep. on the Tel. Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 59-60 (Jan. 23, 2014)). The government's approach "essentially reads the 'authorized investigation' language out of the statute." *Id. at 815-16*.

Finally, we do not accept the government's justification in this case that "the call detail records at issue *here*—the records that suggested that a particular U.S.-based telephone number may have been **[*996]** associated with a foreign terrorist—were clearly relevant to a counterterrorism **[**35]** investigation." Br. of United States 52 (emphasis added). That argument depends on an after-the-fact determination of relevance: once the government had collected a massive amount of call records, it was able to find one that was relevant to a counterterrorism investigation. The problem, of course, is that FISA required the government to make a showing of relevance to a particular authorized investigation *before* collecting the records. *50 U.S.C. § 1861(b)(2)(A) (2006)*.

We hold that the telephony metadata collection program exceeded the scope of Congress's authorization in *section 1861* and therefore violated that section of FISA. *See Clapper, 785 F.3d at 826*.

3.

As a remedy for the FISA violation, defendants ask us to suppress the alleged "fruits" of the unlawful metadata collection, including the evidence from the government's wiretap of ***Moalin***'s phone. Because "suppression is a disfavored remedy," we impose it to remedy a statutory violation "only . . . where it is clearly contemplated by the relevant statute." *United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008)*.[11] To decide whether suppression is clearly contemplated by FISA in this context, we begin with *50 U.S.C. § 1861*, the section under which ***Moalin***'s metadata was collected and which that collection violated.

Section 1861 authorizes the *recipient* of a production **[**36]** order to "challenge the legality" of the order. *Id. § 1861(f)(2)(A)(i)*. But it does not expressly provide for a challenge by the *subject* of the records collected—that is, the person whose records are collected from a third party. Nor does *section 1861*, either as it read at the time relevant to this case, or as it reads now, after amendment by the USA Freedom Act, contain any provision for suppressing in a criminal trial evidence obtained in violation of the section. *Compare 50 U.S.C. § 1861 with 50 U.S.C. § 1861 (2006)*. The remainder of Subchapter IV likewise makes no mention of a suppression remedy.

---

[11] In some circumstances a court may order suppression to remedy the violation of a statute that "enforce[s] constitutional norms," even if the statute does not expressly call for suppression. *United States v. Dreyer, 804 F.3d 1266, 1278 (9th Cir. 2015)*. We decline to impose suppression on that basis in this case for the same reason we conclude suppression would not be warranted were we to decide that the metadata program violated the *Fourth Amendment*. *See supra p. 23*.

The lack of a suppression remedy in section 1861, and in Subchapter IV more generally, is significant because all the other FISA subchapters authorizing intelligence collection do contain a suppression remedy. *See id.* § 1806(g) (Subchapter I, concerning electronic surveillance); *id.* § 1825(h) (Subchapter II, concerning physical searches); *id.* § 1845(g) (Subchapter III, concerning pen registers and trap-and-trace devices); *id.* § 1881e(b) (Subchapter VI, or the FISA Amendments Act, concerning surveillance of persons outside the United States).

Of particular significance is that Congress added Subchapters III and IV to FISA in the same legislation. It chose expressly to authorize a suppression remedy **[**37]** in Subchapter III[12] but not in Subchapter IV. *See Pub. L. No. 105-272, Title VI, §§ 601-602, 112 Stat. 2396, 2404-2412 (1998)*. "[W]here Congress includes particular language in one section of a **[*997]** statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello v. United States, 464 U.S. 16, 23, 104 S. Ct. 296, 78 L. Ed. 2d 17 (1983)* (alteration in original). This presumption is "strongest in those instances in which the relevant statutory provisions were considered simultaneously when the language raising the implication was inserted," as is the case with Subchapters III and IV. *Gomez-Perez v. Potter, 553 U.S. 474, 486, 128 S. Ct. 1931, 170 L. Ed. 2d 887 (2008)* (internal quotation marks omitted). We therefore conclude that suppression is not "clearly contemplated" by section 1861, *Forrester, 512 F.3d at 512*, and that there is no statutory basis for suppressing ***Moalin***'s metadata itself.

Recognizing the gap in Subchapter IV, defendants urge us to rely on the suppression remedy in Subchapter I. *See* 50 U.S.C. § 1806(g). As discussed, the government obtained an order from the FISA Court under Subchapter I authorizing a wiretap of ***Moalin***'s phone, and introduced evidence obtained from the wiretap at trial. Defendants were entitled to "move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that . . . the information was unlawfully **[**38]** acquired." *Id.* § 1806(e). The statute instructs that, if the "district court . . . determines that the surveillance *was not lawfully authorized* . . . it *shall*, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance." *Id.* § 1806(g) (emphases added).

To obtain the ***Moalin*** wiretap order, the government submitted an application to the FISA Court including, among other things, "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power." *50 U.S.C. § 1804(a)(4)(A) (2006)*. The government's application is classified, and the district court denied defendants' request to see it. Nonetheless, defendants assume, based on the public statements of government officials following the Snowden disclosures, *see supra* pp. 13-14, that the application relied at least in part on ***Moalin***'s metadata. Defendants contend that because the metadata was obtained in violation of the "relevance" provision in Subchapter IV, *50 U.S.C. § 1861(b)(2)(A) (2006)*, the evidence obtained from the subsequent wiretap was therefore "unlawfully acquired" for purposes of Subchapter I, *50 U.S.C. § 1806(e)*.

---

[12] Upon finding that the use of a pen register "was not lawfully authorized or conducted," a district court "may . . . suppress the evidence which was unlawfully obtained or derived from the use of the pen register." *50 U.S.C. § 1845(g)(1)*.

Contrary **[**39]** to defendants' assumption, the government maintains that ***Moalin***'s metadata "did not and was not necessary to support the requisite probable cause showing" for the Subchapter I application in this case. Our review of the classified record confirms this representation. Even if we were to apply a "fruit of the poisonous tree" analysis, *see* *Wong Sun, 371 U.S. at 487-88*, we would conclude, based on our careful review of the classified FISA applications and related information, that the FISA wiretap evidence was not the fruit of the unlawful metadata collection. Again, if the statements of public officials created a contrary impression, that impression is inconsistent with the facts presented in the classified record. Because the wiretap evidence was not "unlawfully acquired," suppression is not warranted. *50 U.S.C. § 1806(e)*.

II. Notice of Surveillance Activities

Separately from their contention that the metadata collection violated their *Fourth Amendment* rights, defendants maintain that the *Fourth Amendment* required the government to provide notice to defendants of its collection and use of ***Moalin***'s **[*998]** telephony metadata. They also contend that they were entitled to notice of any additional surveillance, other than FISA Subchapter I surveillance, that the government conducted **[**40]** of them during the course of its investigation.[13]

A.

After defendants were indicted, the government notified them and the district court that it intended to "use or disclose" in "proceedings in this case information obtained or derived from electronic surveillance conducted pursuant to the authority of [FISA]." *See* *50 U.S.C. § 1806(c)* (FISA Subchapter I notice requirement). That information turned out to be recordings and transcripts of defendants' phone calls stemming from the government's wiretap of ***Moalin***'s cell phone under FISA Subchapter I.

The government did not notify defendants that it had collected ***Moalin***'s phone records as part of the metadata program. Defendants learned that after trial—from the public statements that government officials made in the wake of the Snowden disclosures. *See supra* pp. 13-14. Nor did the government provide notice of any additional surveillance, apart from FISA Subchapter I surveillance, it had conducted of defendants. Defendants contend that at least some such surveillance may have occurred, because the email to the linguist produced by the government two days before trial referred to a phone call to ***Moalin*** that had not gone through and therefore presumably would not have been captured **[**41]** by the wiretap of ***Moalin***'s phone. *See supra* p. 13. According to defendants, any additional surveillance of ***Moalin***, depending on when it began (and regardless of whether it targeted ***Moalin***), may have provided information used in

[13] The government asserts that defendants forfeited their argument that they were entitled to notice of the metadata collection by failing to raise it before the district court. Defendants adequately raised the issue in their motion for a new trial, arguing that they were "not provided any notice" of the metadata collection and that the government's response to defendants' motion to suppress FISA surveillance was therefore incomplete. The government does not address defendants' argument that they were entitled to notice of any additional surveillance the government conducted.

the wiretap applications or may otherwise have contributed to the evidence used by the government at trial.

Just months after defendants' convictions, news articles in the wake of the Snowden disclosures revealed that the government had been using evidence derived from foreign intelligence surveillance in criminal prosecutions without notifying the defendants of the surveillance. Five years earlier, Congress had passed the FISA Amendments Act ("FAA"), which provided congressional authorization for a surveillance program the government had previously conducted outside the auspices of FISA. *Pub. L. No. 110-261, 122 Stat. 2436 (2008)*; *see* Kris & Wilson, *supra* note 5, § 17:1. The FAA permits the government to conduct electronic surveillance of people it believes are located outside the United States without using the procedures required by FISA Subchapter I. *50 U.S.C. §§ 1881a*, *1881b*, *1881c*. If the government intends to use evidence "obtained or derived from" FAA surveillance in a criminal prosecution, however, it must provide notice to the defendants as required by FISA Subchapter **[**42]** I. *Id. §§ 1806(c)*, *1881e(a)(1)*. In 2013, it came to light that the government had been using evidence derived from FAA surveillance in criminal prosecutions without providing the mandated notice. *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, http://nyti.ms/1r7mbDy.

[*999] Additionally, the government conducts other foreign intelligence surveillance outside the United States, beyond the scope of FISA or the FAA, under Executive Order 12,333. *See* Exec. Ord. No. 12,333, as amended by Exec. Ord. Nos. 13,284 (2003), 13,355 (2004), and 13,470 (2008); Kris & Wilson, *supra* note 5, §§ 2:7, 17:1. Following the passage of the FAA, Executive Order 12,333 no longer authorizes surveillance targeting U.S. persons, but such persons' communications and metadata may be incidentally collected.[14] *See* Kris & Wilson, *supra* note 5, § 17:19. Executive Order 12,333 does not contain any notice requirement.

B.

The *Fourth Amendment* requires that a person subject to a government search receive notice of the search, absent "exigent circumstances." *Berger v. State of New York, 388 U.S. 41, 60, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967)*; *see United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986)*. Courts have excused *advance* notice in the wiretapping context for a practical reason: if the subject of a wiretap were "told in advance that federal officers intended to record his conversations, the point of making such recordings would obviously [be] lost." *Katz, 389 U.S. at 355 n.16*. In such circumstances, the government must provide a "constitutionally adequate **[**43]** substitute for advance notice." *Dalia v. United States, 441 U.S. 238, 248, 99 S. Ct. 1682, 60 L. Ed. 2d 177 (1979)*. *Dalia* explained that the *Wiretap Act*, which governs the use of electronic surveillance in criminal investigations, meets this requirement by instructing that "once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance." *Id.* (citing *18 U.S.C. § 2518(8)(d)*); *see United States v. Donovan, 429 U.S. 413, 429 n.19, 97 S. Ct. 658, 50 L. Ed. 2d 652 (1977)*.

---

[14] Executive Order 12,333 and FISA contain similar definitions of "United States person." Both definitions include U.S. citizens and permanent residents. *See 50 U.S.C. § 1801(i)*; Exec. Ord. No. 12,333, as amended, § 3.5(k).

The government argues that *Berger* and *Dalia* are inapposite here because they dealt with ordinary criminal investigations, and the *Fourth Amendment* requirements are different in the foreign intelligence context. The government points to *United States v. Cavanagh*, which quoted *United States v. United States District Court (Keith), 407 U.S. 297, 322-23, 92 S. Ct. 2125, 32 L. Ed. 2d 752 (1972)*, for the proposition that a different standard may be compatible with the *Fourth Amendment* in the intelligence-gathering context if it is "reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." *807 F.2d 787, 790 (9th Cir. 1987)*. *Cavanagh* held that "FISA satisfies the constraints the *Fourth Amendment* places on foreign intelligence surveillance conducted by the government." *Id.* For our purposes, the essential insight of *Cavanagh* is that even if the *Fourth Amendment* applies differently in the foreign intelligence context, it still *applies*, at least if U.S. persons are involved.[15]

Cavanagh ***[**44]*** did not address the *Fourth Amendment's* notice requirement, **[*1000]** but the insight we glean from it bears on our analysis here: because the *Fourth Amendment* applies to foreign intelligence investigations, U.S. criminal defendants against whom the government uses evidence obtained or derived from foreign intelligence surveillance may have *Fourth Amendment* rights to protect. The principal remedy for a *Fourth Amendment* violation is the exclusionary rule: a criminal defendant may seek suppression of evidence obtained from an unlawful search or seizure, as well as of the "fruits" of that evidence—additional evidence to which it led. *See Wong Sun, 371 U.S. at 488*. But criminal defendants who have no knowledge that a potentially unconstitutional search has played a part in the government's case against them have no opportunity to vindicate any *Fourth Amendment*-protected rights through suppression.

Notice is therefore a critical component of the *Fourth Amendment* in the context of a criminal prosecution. And although the *Fourth Amendment* may apply differently to foreign intelligence surveillance than to searches undertaken in ordinary criminal investigations, notice of a search plays the same role in the criminal proceeding: it allows the defendant to assess whether the surveillance complied with the *Fourth Amendment's* requirements, whatever the parameters **[**45]** of those requirements are. Indeed, the Supreme Court has recognized that the notice provisions in FISA and the FAA serve precisely that function. *See Amnesty Int'l USA, 568 U.S. at 421* & n.8.

At the same time, the need for secrecy inherent in foreign intelligence investigations justifies a more circumscribed notice requirement than in the ordinary criminal context. *See* Kris & Wilson, *supra* note 5, § 29:2 (discussing the need for secrecy). Whereas the Wiretap Act requires notice at the end of an investigation regardless of whether an indictment is filed, *18 U.S.C. § 2518(8)(d)*, the FISA and FAA notice provisions are more limited, requiring notice only when the "Government intends to enter into evidence or otherwise use or disclose in any trial . . . or other proceeding in or before any court . . . or other authority of the United States, against an

[15] In some circumstances, surveillance targeting a non-U.S. person does not require a warrant, even if a U.S. person's communications are incidentally collected. *See United States v. Mohamud, 843 F.3d 420, 439-41 (9th Cir. 2016)*. But we have assumed that, even in such circumstances, the incidental collection affects the *Fourth Amendment* rights of the U.S. person, *id. at 441 n.26*, and therefore the search must be "reasonable in its scope and manner of execution," *id. at 441* (quoting *Maryland v. King, 569 U.S. 435, 448, 133 S. Ct. 1958, 186 L. Ed. 2d 1 (2013)*).

aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter," 50 U.S.C. § 1806(c); see id. §§ 1825(d) (physical search), 1845(c) (pen register and trap-and-trace surveillance); 1881e(a)(1) (FAA).[16] According to the Senate Judiciary Committee Report accompanying FISA, Congress was aware that it was "depart[ing] from traditional Fourth Amendment criminal procedures," but it concluded **[**46]** that the "need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination" of the "requirement of subsequent notice to the surveillance target . . . *unless the fruits are to be used against him in legal proceedings*." S. Rep. No. 95-701, at 11-12 (1978) (emphasis added).

At a minimum, then, the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities. *See* Dalia, 441 U.S. at 248; Berger, 388 U.S. at 60.

This constitutional notice requirement applies to surveillance conducted under FISA and the FAA, which codify the **[*1001]** requirement with respect to several types of surveillance. 50 U.S.C. §§ 1806(c), 1825(d), 1845(c), 1881e(a)(1). It also applies to surveillance conducted under other foreign intelligence authorities, including Executive Order 12,333 and the FAA's predecessor programs. Indeed, the notice requirement is of particular importance with regard to these latter, non-statutory programs precisely because these programs lack the statutory protections included in FISA. Where statutory protections are lacking, the Fourth Amendment's reasonableness requirement takes on importance **[**47]** as a limit on executive power, and notice is necessary so that criminal defendants may challenge surveillance as inconsistent with that requirement.

We emphasize that notice is distinct from disclosure. Given the need for secrecy in the foreign intelligence context, the government is required only to inform the defendant that surveillance occurred and that the government intends to use information obtained or derived from it. Knowledge of surveillance will enable the defendant to file a motion with the district court challenging its legality. If the government avers that disclosure of information relating to the surveillance would harm national security, then the court can review the materials bearing on its legality *in camera* and *ex parte*. *See, e.g.*, 50 U.S.C. § 1806(f) (allowing *in camera, ex parte* review of the legality of electronic surveillance under FISA Subchapter I if "the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States").

C.

Here, assuming without deciding that the government should have provided notice of the metadata collection to defendants, the government's failure to do so did not prejudice defendants. **[**48]** Defendants learned of the metadata collection, albeit in an unusual way, in

[16] An "aggrieved person" is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." *Id.* § 1801(k).

time to challenge the legality of the program in their motion for a new trial and on appeal. *See Mohamud, 843 F.3d at 436*. The "purpose of the [notice] rule has thereby been vindicated." *New York v. Harris, 495 U.S. 14, 20, 110 S. Ct. 1640, 109 L. Ed. 2d 13 (1990)*.

Defendants also contend they should have received notice of any other surveillance the government conducted of ***Moalin***, noting that there is some reason to think it did conduct other surveillance. *See supra* p. 35. Based on our careful review of the classified record, we are satisfied that any lack of notice, assuming such notice was required, did not prejudice defendants. Our review confirms that on the particular facts of this case, information as to whether surveillance other than the metadata collection occurred would not have enabled defendants to assert a successful *Fourth Amendment* claim. We therefore decline to decide whether additional notice was required.

III. *Brady* Claims

Defendants contend that the government violated their rights under *Brady v. Maryland, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963)*, by failing to produce exculpatory evidence. *Brady* held that the *Due Process Clause* requires prosecutors to produce "evidence favorable to an accused upon request . . . where the evidence is material either to guilt or to punishment." *Id. at 87*. "[E]vidence **[**49]** is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *United States v. Bagley, 473 U.S. 667, 682, 105 S. Ct. 3375, 87 L. Ed. 2d 481 (1985)*.[17] We review de novo whether a **[*1002]** *Brady* violation has occurred. *United States v. Cano, 934 F.3d 1002, 1022 n.14 (9th Cir. 2019)*.

The government submitted five requests for a protective order under the Classified Information Procedures Act ("CIPA"), which allows the court to "authorize the United States to delete specified items of classified information from documents" provided to the defendant in discovery, "to substitute a summary of the information," or "to substitute a statement admitting relevant facts that the classified information would tend to prove." 18 U.S.C. App. 3 § 4. The district court carefully reviewed the classified documents submitted by the government to determine whether they contained information required to be disclosed under *Brady*. The court held *in camera, ex parte* hearings; asked defendants for a sealed memorandum identifying their legal theories to aid the court in assessing materiality; requested additional classified documents from the government; and issued sealed orders discussing all the withheld information in detail as to whether it met the *Brady* standard. For information **[**50]** that it determined was both favorable to defendants and material, the court ordered the government to provide substituted statements that conveyed the material substance of the information.

---

[17] We note that, in general, the *Brady* materiality inquiry might unfold differently if it were analyzed from the perspective of the prosecution at the time of the pretrial decision whether to disclose. But our case law has treated the inquiry on appeal as retrospective: we analyze the withheld evidence in the "context of the entire record," including the "evidence each side presented at trial," to decide whether the failure to disclose favorable evidence "undermines confidence in the outcome of the trial." *United States v. Jernigan, 492 F.3d 1050, 1054 (9th Cir. 2007)* (en banc).

On appeal, defendants assert, first, that the government was required to produce the evidence underlying an FBI Field Intelligence Group Assessment ("FIG Assessment"), and a 2008 General Assessment Questionnaire completed by the Somali linguist who interpreted the intercepted calls. The FIG Assessment evaluated "***Moalin***'s motivation for providing financial support to al-Shabaab," and the questionnaire included a summary of ***Moalin***'s "personality, behavior, [and] attitudes."

The government maintains that both documents present opinions based only on the intercepted phone calls, which the government provided in full to defendants in discovery. Having carefully reviewed the classified record, we agree with the district court that there is "no reason to suspect or speculate that the Government may have faltered in its *Brady* obligations" in this regard.

Second, defendants contend the government was required to produce any favorable, material evidence relating to the FISA surveillance or to the previously **[**51]** terminated investigation of ***Moalin***. Based on our review of the classified record and of the district court's extensive sealed orders covering *Brady* issues, neither the classified FISA materials nor the file concerning the previously terminated investigation of ***Moalin*** contained favorable, material information. More generally, we are satisfied that the district court's several determinations regarding *Brady* issues in its sealed orders were correct.

IV. Evidentiary Challenges

Defendants contend that certain evidentiary rulings by the district court impermissibly prejudiced the defense.

A.

At trial, defense witness Halima Ibrahim testified to ***Moalin***'s support of her organization, IIDA, which was dedicated to the **[*1003]** education of girls and the advancement of women's rights in Somalia. Ibrahim testified that IIDA was still in existence; that ***Moalin*** provided financial support to IIDA and allowed the organization to use his house; and that IIDA's goals were antithetical to al-Shabaab's. The district court did not, however, permit Ibrahim to testify that ***Moalin*** helped organize a conference in Somalia in 2009 addressing the kidnapping of aid workers, after which al-Shabaab announced on the radio that **[**52]** the organizers of the conference were against al-Shabaab. The district court concluded that this evidence was minimally probative as to ***Moalin***'s intent during the time period relevant to the indictment, 2007 to 2008. Defendants challenge this ruling.

An erroneous evidentiary ruling provides grounds for reversal if the ruling "more likely than not affected the verdict." *United States v. Pang, 362 F.3d 1187, 1192 (9th Cir. 2004)*. Here, any error on the part of the district court was harmless. A significant amount of evidence in the record demonstrated that ***Moalin*** was at times affiliated with causes that took positions disapproved by al-Shabaab, including Ibrahim's testimony regarding ***Moalin***'s support of projects benefitting girls and the government's stipulation that one of the charities with which ***Moalin*** was involved was opposed to al-Shabaab. To the degree the excluded evidence had any pertinence to whether ***Moalin*** was ideologically aligned with al-Shabaab in 2007 and 2008,

it served at best marginally to reinforce Ibrahim's uncontested testimony directly concerning the relevant time period. We cannot say that the exclusion of Ibrahim's testimony regarding the 2009 conference "more likely than not affected the verdict." *See id.*

B.

Before trial, **[**53]** ***Moalin*** and his co-defendants moved to take depositions of defense witnesses residing in Somalia who could not or would not travel to the United States to testify. The court ultimately granted defendants' motion to the extent the depositions could be taken in neighboring Djibouti.[18]

One proposed defense witness was Farah Shidane, also called Farah Yare. The indictment against defendants listed four transfers of funds for which "Farah Yare" (or, in one instance, "farahyare") was named as the recipient on Shidaal Express's transaction register. Defendants anticipated that Shidane would testify that he was part of the local administration for ***Moalin***'s home region in Somalia, that he fought against al-Shabaab, and that the money he received from defendants was used for humanitarian purposes.

After the government identified Shidane as an unindicted co-conspirator in the case, defendants sought an order compelling the government to give Shidane "safe passage," *i.e.*, a guarantee that it "would not arrest or otherwise detain [him] because he appeared at the deposition in Djibouti." Alternatively, defendants sought authorization to depose Shidane in Somalia via videoconference. The district court **[**54]** denied both requests.

Shidane refused to travel to Djibouti for his scheduled deposition. Depositions of seven other witnesses proceeded in Djibouti, and the defense presented six of the videotaped depositions to the jury. The defense elicited testimony at trial that Shidane was involved in the regional administration for ***Moalin***'s home region and presided over a drought relief committee. **[*1004]** Ultimately, the government did not rely on the transfers to Shidane as part of the case it submitted to the jury, and counsel for the prosecution told the jury that "the government is not alleging that Farah Yare was part of al-Shabaab."

Defendants challenge the district court's denial of their request for "safe passage" for Shidane and of their motion to conduct his deposition via videoconference.[19] We first address the request for "safe passage."

Under certain circumstances, due process may require a court to compel the prosecution to grant, at least, *use* immunity.[20] *See* 18 U.S.C. § 6002; *Straub, 538 F.3d at 1148*. Use immunity guarantees witnesses that their testimony will not be used against them in a criminal case (except that it does not protect against a prosecution for perjury). *See* 18 U.S.C. § 6002. A

---

[18] The government represented that it would not be safe for prosecutors to travel to Somalia.

[19] After Shidane failed to appear at his deposition in Djibouti, defendants renewed their motion to depose him by video. The district court again denied the motion.

[20] Whether a district court erred by refusing to grant use immunity is a mixed question of law and fact that we review de novo. *United States v. Straub, 538 F.3d 1147, 1156 (9th Cir. 2008)*.

request to compel immunity implicates "important separation **[**55]** of powers concerns" because the court, in granting the request, "impede[s] on the discretion of the executive branch" to decide whether to prosecute a case. *Straub, 538 F.3d at 1156*. Given these concerns, due process requires a court to grant use immunity to a defense witness only when the defense establishes that the testimony would be relevant and that:

> (a) the prosecution intentionally caused the defense witness to invoke the *Fifth Amendment* right against self-incrimination with the purpose of distorting the fact-finding process; or (b) the prosecution granted immunity to a government witness in order to obtain that witness's testimony, but denied immunity to a defense witness whose testimony would have directly contradicted that of the government witness, with the effect of so distorting the fact-finding process that the defendant was denied his due process right to a fundamentally fair trial.

Id. at 1162.

Defendants' request for immunity for Shidane from arrest abroad was somewhat distinct from a request for use immunity and may implicate additional separation of powers concerns. Even assuming defendants were required to satisfy only the *Straub* test, however, that test was not met.

Defendants contend they met the first prong because **[**56]** the government had named Shidane as "uncharged coconspirator #1." But there is no indication that the government "intentionally caused [Shidane] to invoke the *Fifth Amendment* right against self-incrimination with the purpose of distorting the fact-finding process." *Straub, 538 F.3d at 1162*. The government referred to "uncharged co-conspirator #1" in the October 2010 indictment and subsequent indictments, suggesting the government had long considered Shidane a person of interest and did not change its position to discourage Shidane's testimony. And the district court found no evidence "to suggest that the Government interfered in any manner with Mr. Shidane's ability to appear at his deposition." Defendants were not entitled to compel safe passage for Shidane.

As for defendants' request to take a video deposition of Shidane in Somalia, a court may grant a motion to depose a prospective witness, including by **[*1005]** video, "because of exceptional circumstances and in the interest of justice." *Fed. R. Crim. P. 15(a)(1)*; *see United States v. Yida, 498 F.3d 945, 960 (9th Cir. 2007)*. Courts consider, "among other factors, whether the deponent would be available at the proposed location for deposition and would be willing to testify," as well as "whether the safety of United States officials would be compromised by **[**57]** going to the foreign location." *United States v. Olafson, 213 F.3d 435, 442 (9th Cir. 2000)*. We review the district court's denial of defendants' motion for abuse of discretion. *United States v. Omene, 143 F.3d 1167, 1170 (9th Cir. 1998)*.

The district court reasoned that permitting defendants to depose Shidane by video in Somalia would not be in the interests of justice because defendants could not show that there would be procedures in place to ensure the reliability and trustworthiness of Shidane's testimony. Specifically, defendants could not show that an "oath in Somalia is subject to penalties of perjury and judicial process like those available in the United States." In light of these concerns, the district court did not abuse its discretion in denying defendants' motion.

Even if the district court did abuse its discretion, any error, in denying either defendants' request for "safe passage" or their request to depose Shidane by video, was harmless. Shidane's anticipated testimony could have marginally supported the defense's showing that ***Moalin*** contributed to humanitarian causes, including those opposed to al-Shabaab. But, as we have noted, there was considerable other evidence in the record that ***Moalin*** contributed to a variety of humanitarian causes. Additionally, the government made clear it **[**58]** was not alleging that Shidane was part of al-Shabaab, and the government did not rely on the money transfers to Shidane in its arguments to the jury. In short, the district court's refusal to compel "safe passage" or to permit a video deposition in Somalia did not prejudice the defense.

C.

Defendants' final evidentiary challenge involves testimony at trial relating to the so-called "Black Hawk Down" incident. The district court permitted the government's expert to discuss briefly a 1993 incident in which two U.S. helicopters were shot down in Mogadishu by a group other than al-Shabaab. Defendants argue that the testimony's probative value was substantially outweighed by prejudice to defendants.

The district court did not abuse its discretion in permitting the government expert's very brief testimony regarding the incident. On direct examination, the expert said only that "18 American soldiers were killed, several dozen injured, an estimated 1,000 Somalis were casualties of that clash, and it was the event that led the United States government to withdraw its forces the following year." This brief and matter-of-fact testimony was delivered as part of a long chronology detailing Somalia's **[**59]** recent history, which both parties agreed was generally relevant. Defense counsel revisited the incident on cross-examination, asking about the number of Somali casualties, and also mentioned it in passing during closing argument. The expert's testimony was not tied to defendants or to al-Shabaab in any way and was therefore unlikely to have prejudiced the jury against defendants. So, even if the district court did abuse its discretion in admitting the testimony, the error was harmless. *See* *Pang, 362 F.3d at 1192*.

D.

Defendants contend that the evidentiary rulings just discussed, even if not **[*1006]** prejudicial on their own, constituted cumulative error. To the extent we have found the claimed errors of the district court harmless, "we conclude that the cumulative effect of such claimed errors is also harmless because it is more probable than not that, taken together, they did not materially affect the verdict." *United States v. Fernandez, 388 F.3d 1199, 1256-57 (9th Cir. 2004)*. Even if the district court did err in any respect, its rulings did not affect any essential element of the case. Neither ***Moalin***'s involvement in the 2009 conference nor Shidane's additional testimony about ***Moalin***'s humanitarian efforts would have undermined the validity of the government's key evidence—the **[**60]** recorded calls and the money transfer records. The omission of that additional testimony, combined with the brief discussion of the Black Hawk Down incident, did not significantly undercut the persuasiveness of the defense. So the evidentiary rulings do not support a determination of cumulative error.

V. Sufficiency of the Evidence Against Issa Doreh

Defendant Issa Doreh challenges the sufficiency of the evidence to support the jury's verdict that he was guilty of Counts One (conspiracy to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a)), Two (conspiracy to provide material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1)), Three (conspiracy to launder monetary instruments in violation of 18 U.S.C. § 1956(a)(2)(A) and (h)), and Five (providing or aiding and abetting the provision of material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1) and (2)). We review de novo whether sufficient evidence supports a conviction, asking whether, "viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." United States v. Chung, 659 F.3d 815, 823 (9th Cir. 2011).

To prove Count One, the prosecution was required to prove beyond a reasonable **[**61]** doubt that: (1) Doreh entered into a conspiracy; (2) the objective of the conspiracy was to provide material support or resources; and (3) he knew and intended that the provision of such material support or resources would be used in preparing for, or in carrying out, a conspiracy to kill persons in a foreign country (18 U.S.C. § 956) or a conspiracy to use a weapon of mass destruction outside of the United States (18 U.S.C. § 2332a(b)). 18 U.S.C. § 2339A(a); *see* United States v. Hassan, 742 F.3d 104, 112 (4th Cir. 2014). To prove Count Two, the prosecution had to prove beyond a reasonable doubt that Doreh entered into a conspiracy to provide material support or resources to al-Shabaab, knowing that al-Shabaab was a designated terrorist organization or that it engaged in terrorist activity. *See* 18 U.S.C. § 2339B(a)(1). To prove Count Three, the prosecution had to prove beyond a reasonable doubt that Doreh entered into an agreement to transfer funds with an "intent to promote the carrying on of specified unlawful activity," namely, the provision of material support to foreign terrorists and a foreign terrorist organization, with intent to promote a conspiracy to kill persons in a foreign country. *Id.* § 1956(a)(2)(A) and (h). Finally, to prove Count Five, the government had to prove beyond a reasonable doubt that Doreh either knowingly **[**62]** provided material support and resources to a foreign terrorist organization or that he "knowingly and intentionally aided" in the commission of that offense. 18 U.S.C. §§ 2, 2339B(a)(1).

None of the three conspiracy counts required the prosecution to prove that Doreh committed an overt act in furtherance of **[*1007]** the conspiracy. *See id*. §§ 2339A, 2339B(a)(1); Whitfield v. United States, 543 U.S. 209, 219, 125 S. Ct. 687, 160 L. Ed. 2d 611 (2005); United States v. Stewart, 590 F.3d 93, 114-16 (2d Cir. 2009). The prosecution also did not have to prove that Doreh "kn[ew] all the conspirators, participated in the conspiracy from its beginning, participated in all its enterprises, or [knew] all its details." United States v. Torralba-Mendia, 784 F.3d 652, 664 (9th Cir. 2015) (internal quotation marks and citations omitted).

Viewing the evidence in the light most favorable to the prosecution, a rational jury could conclude beyond a reasonable doubt that the elements of Counts One, Two, Three, and Five were satisfied.

Doreh maintains that the government could not prove that "Shikhalow"—the person identified on the calls with ***Moalin***—was actually Aden Hashi Ayrow, the important al-Shabaab figure. The

call transcripts introduced by the government reflect calls between ***Moalin*** and Shikhalow from December 21, 2007, to April 25, 2008. It can be inferred from ***Moalin***'s conversations with Shikhalow and others that "Shikhalow" was a code name for Ayrow. On December **[**63]** 30, 2007, an unidentified man asked ***Moalin*** whether "Aden Ayrow" was the leader of "these youth"; "al-Shabaab" means "the youth" in Arabic. ***Moalin*** replied that while Aden Ayrow had superiors, he was "involved in it extensively." On January 3, 2008, ***Moalin*** spoke to Shikhalow and then told an unidentified man on a call beginning about half an hour later that "right now, when . . . you were calling me . . . I was talking to the man who is in charge of the youth." Later, on January 20, 2008, Shikhalow told ***Moalin*** that "we, the Shabaab, have a political section, a military section and a missionary section." Further, on February 17, 2008, an acquaintance of ***Moalin***'s told ***Moalin*** he had "heard that . . . [***Moalin***'s] friend, Aden Hashi Ayrow, [was] in Dhusa Mareeb . . . and [was] taking part in the fighting . . . and [was] pleading for support. . . ."

The transcripts also indicate that Doreh was aware of Shikhalow's identity as Aden Ayrow. Ayrow died in a U.S. missile strike on May 1, 2008. That same day, ***Moalin*** learned from an acquaintance that "the house where Shikhalow . . . used to stay" was targeted. ***Moalin*** then learned from another acquaintance that a missile was dropped on a house "thought **[**64]** to be inhabited by the main man." ***Moalin*** then called M. Mohamud and told him that "mainly the news is that even Majadhub is among [the people who are gone]." "Majadhub" was another name for Shikhalow. Lastly, ***Moalin*** called Doreh and told him: "[T]hat man is gone . . . . That news is highly reliable—that he is gone. . . . [T]he people whom he was working with reported that news." Doreh responded: "You mean Aden?" ***Moalin*** replied: "Yes."

Further, a rational juror could conclude beyond a reasonable doubt that Doreh was aware of Shikhalow's involvement with violent activity. On December 21, 2007, ***Moalin*** discussed with Shikhalow the money Shikhalow needed for the remainder of the month. ***Moalin*** told Shikhalow that he would talk to "the Saleban clan cleric whom you talked to, by the name of Sheikh Issa, who is a very dear man." (Issa is Doreh's first name, and ***Moalin*** addressed him directly as "Sheikh Issa.") Minutes after talking to Shikhalow, ***Moalin*** called Doreh and told him that the "cleric whom you spoke with the other day" had just called and requested money. ***Moalin*** told Doreh that the money was "need[ed] for our forces stationed" in the "places where the fighting are [sic] going on." A **[**65]** few months later, on April 21, 2008, Doreh told ***Moalin*** and another man that "whoever fights against the aggressive non-Muslims . . . will be victorious" and that "today **[*1008]** there is no better cause for a person . . . than to be martyr for his country, land and religion." When Doreh learned of "Aden's" death, he told ***Moalin*** that the "question is not how he died but the important thing is what he died for[:] . . . the religion of Islam . . . ."

While the transcripts do not include direct conversations between Doreh and Shikhalow, they describe Doreh's involvement with ***Moalin*** and others in transferring funds from San Diego to Shikhalow's organization in Somalia, sometimes using names Doreh knew were invented. The funds were transferred by Shidaal Express, the hawala where Doreh worked. The transactions at issue, totaling $10,900, took place in January, February, April, July, and August of 2008.

As described above, ***Moalin*** informed Shikhalow on December 21, 2007, that ***Moalin*** would handle the sending of funds to Shikhalow "with the . . . cleric whom you talked to, by the name of Sheikh Issa." On that call, Shikhalow told ***Moalin*** that he needed $3,160 for the remainder of the month. Minutes later, **[**66]** ***Moalin*** called Doreh and told him that "[t]he cleric whom you spoke

with the other day" had stated that "an amount of . . . $3600.00 . . . is needed" for the "forces stationed around" "where the fighting are [sic] going on." ***Moalin*** also told Doreh that he had been told that "the most we spend for any one place is $4000.00." ***Moalin*** called Doreh again on December 28, 2007, telling him that "[t]he men requested that we throw something to them for this month" and asking if Sheikh Mohamed had fallen behind schedule. Doreh told ***Moalin*** that he would speak with Sheikh Mohamed about the issue if he saw Sheikh Mohamed that day. ***Moalin*** called Sheikh Mohamed later on December 28, 2007, and received Sheikh Mohamed's promise that he would "complete the task, which pertains to the men, tomorrow. . . ." On January 1, 2008, Shidaal Express transferred two installments of $1,950 (totaling $3,900) to "yusuf mohamed ali." On January 3, 2008, Shikhalow told ***Moalin***: "[W]e received the three."

Moalin and Shikhalow had a long discussion on the morning of January 20, 2008. Later that day,[21] ***Moalin*** told an acquaintance: "[T]he gentlemen [sic] called me this morning. . . . [W]e had a heated debate. He said . . . **[**67]** ']We will use what you give us for bullets and drinking-water for the people. So, don't hold back anything.'" On February 3, 2008, ***Moalin*** asked Shikhalow for news. In response, Shikhalow told ***Moalin***: "You are running late with the stuff. Send some and something will happen." On February 9, 2008, Doreh called ***Moalin*** and told him: "We have sent it." When ***Moalin*** asked whether it was "the one for the youth . . . I mean the orphans or was [sic] the other," Doreh told ***Moalin*** it was "the Dhunkaal one . . . [y]es, two." The Shidaal Express Transaction Records note two transfers totaling $2,000 sent on February 13, 2008, from "dhunkaal warfaa" to "YUSUF MOHAMED ALI." On February 14, 2008, ***Moalin*** spoke to Shikhalow and asked him whether he had "receive[d] Dhunkaal's stuff" in "two pieces" with the name of "Yusuf Mohamed Ali" listed as the receiver. Shikhalow asked if the amount was $2,000, and ***Moalin*** confirmed the amount was correct.

On April 23, 2008, ***Moalin*** called Sheikh Mohamed and asked: "Did Dhunkaal go?" Upon hearing that "Dhunkaal left," ***Moalin*** asked Sheikh Mohamed for details about "where . . . Dhunkaal [went]," and whether "it went to the same name" for the "one whom it is addressed **[**68]** to." Nine minutes **[*1009]** after this conversation began, ***Moalin*** spoke to Doreh and asked him multiple questions about "the name that you used for Dhunkaal" and "the name of the sender," explaining that he had just spoken to Sheikh Mohamed and thought "you used the wrong name." Doreh told ***Moalin***: "He told me the sender is the same as the name of [sic] previous person." On another call a few minutes later, Doreh, ***Moalin***, and Abdirizak, the manager of Shidaal Express, went over the details of the sender, receiver, and location of receipt. Doreh told ***Moalin***: "I made Abdiweli Ahmed as the person sending it"; "the man who is receiving the money" was "Dhunkaal Mohamed Yusuf"; and the location "we sent it to [was] Bakara." When ***Moalin*** asked to change to location to Dhuusa Mareeb, Doreh told ***Moalin***: "Then it will be changed. . . . It is settled. We will transfer it there."

Moalin learned from Shikhalow on April 25, 2008, that Shikhalow had received $1,900. ***Moalin*** called Sheikh Mohamed less than an hour later and asked "how many stones" they had sent to "Majadhub." After learning that "three stones" had been sent, ***Moalin*** told Sheikh Mohamed that Shikhalow had received "[t]wo stones minus one." Sheikh **[**69]** Mohamed told ***Moalin***: "It was sent in installments. That is what they did." Later on April 25, 2008, ***Moalin*** called Abdirizak and

[21] The second transcript is dated January 21 (Universal Time Coordinated), but it was still the afternoon of January 20 in San Diego.

asked whether "[t]hat issue with [] Dhunkaal" had been sent in two installments. Abdirizak confirmed that there were two installments: "[O]ne was for 19 and the other for 11." Abdirizak noted that the second installment was "still outstanding," that the recipient was "Mohamed Yusuf Dhunkaal," that the sender was "Sahra Warsame," and that the location was "Dhusa Mareeb." The Shidaal Express Transaction Records note a transfer of $1,900 on April 23, 2008, from "abdiwali ahmed" to "DUNKAAL MOHAMED YUSUF" as well as a transfer of $1,100 on April 25, 2008, from "Zahra warsame" to "mohamed yusuf dunkaal"; both transfers record a receiver city of "DHUUSAMAREEB."

After Ayrow's death, ***Moalin*** told an acquaintance on May 8, 2008: "If the man that we used to deal with is gone—I mean—that the assistance and the work that we were performing—we want it not to stop." ***Moalin*** appears to have been asking the acquaintance to connect him to someone else so that ***Moalin*** could continue supporting al-Shabaab: "So now that man is gone we want to have contact with another man God willing. **[**70]** So we can continue the assistance as before." On July 11, 2008, ***Moalin*** made contact, apparently for the first time, with Omar Mataan. After learning that the man on the phone was Mataan, ***Moalin*** told him: "Man, our contact got interrupted. You know that I had contact with the scholar, don't you? . . . After the man left the scene, the whole contact was interrupted, you know?" Mataan told ***Moalin*** that he would be in Dhusa Mareeb until "the Friday after next Friday," or July 25, 2008. ***Moalin*** then told Mataan: "It will come under the name of the account we used before, which was Dhunkaal. . . . [A]nd I will write your name as it is: Omar Mataan." On July 18, 2008, ***Moalin*** told an unidentified man that Omar Mataan was "one of the guys in the region and one of the youth."

On July 22, 2008, ***Moalin*** told Mataan: "[W]e threw two cartons addressed to . . . your name, Omar Mataan. . . . I sent it to Dhusa Mareeb." The next day, ***Moalin*** told Doreh: "[A]sk your friend if the stuff reached the children." Doreh replied: "I personally checked the whole thing. . . . That money had [sic] exchanged hand." After a segment of the conversation unintelligible to the interpreter, ***Moalin*** told Doreh: "No, we are **[**71]** talking about something else now, about the youngsters; . . . there were two cartons that I allocated for them. . . ." Doreh responded throughout **[*1010]** with "yes" and finally told ***Moalin*** that the two of them should meet.

On July 24, 2008, Mataan reported to ***Moalin*** that he had "received the stuff" and that it was "1, 6 eh 5, 0." ***Moalin*** told Mataan: "It should have been two cartons. . . . I understood that you received 1, 6, 5, 0 and still short of 3, 5, 0." The Shidaal Express Transaction Records note a transfer of $1,650 on July 23, 2008, from "Kulan Muhumed" to "Omer Mataan" with a receiver city of "DHUUSAMAREEB," and a further transfer of $350 on August 5, 2008, from "Hashi mohamed" to "Omer matan" with a receiver city of "DHUUSAMAREEB."

Viewing the evidence in the light most favorable to the prosecution, a reasonable jury could have concluded beyond a reasonable doubt that Doreh entered into an agreement to provide material support, knowing the support would be used in preparing for, or in carrying out, a conspiracy to kill persons in a foreign country, *see* 18 U.S.C. § 2339A; that he entered into an agreement to provide material support to al-Shabaab, knowing that al-Shabaab was tied to terrorism, *see id* ***[**72]*** . § 2339B(a)(1); that he entered into an agreement to transfer funds with an intent to promote the provision of material support to foreign terrorists and a foreign terrorist organization, intending to promote a conspiracy to kill persons in a foreign country; *see id*. § 1956(a)(2)(A) and (h); and that he knowingly aided in the provision of material support to a

designated foreign terrorist organization, *see id*. §§ 2, 2339B(a)(1). We therefore affirm Doreh's convictions.

CONCLUSION

Defendants' convictions are **AFFIRMED**.

End of Document

APPENDIX B: Denial of Petitions for Rehearing and Petitions for rehearing en banc, filed February 27, 2025

United States v. Moalin

United States Court of Appeals for the Ninth Circuit

February 27, 2025, Filed

No. 13-50572, No. 13-50578, No. 13-50580, No. 14-50051

Reporter
2025 U.S. App. LEXIS 4643 *

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BASAALY SAEED ***MOALIN***, AKA Basal, AKA Muse Shekhnor Roble, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MOHAMED MOHAMED MOHAMUD, AKA Mohamed Khadar, AKA Sheikh Mohamed, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. ISSA DOREH, AKA Sheikh Issa, Defendant-Appellant.UNITED STATES OF AMERICA, Plaintiff-Appellee, v. AHMED NASIR TAALIL MOHAMUD, Defendant-Appellant.

Prior History: [*1] D.C. No. 3:10-cr-04246-JM-1, D.C. No. 3:10-cr-04246-JM-2, D.C. No. 3:10-cr-04246-JM-3, D.C. No. 3:10-cr-04246-JM-4. Southern District of California, San Diego.

United States v. ***Moalin***, 973 F.3d 977, 2020 U.S. App. LEXIS 28119, 2020 WL 5225704 (9th Cir. Cal., Sept. 2, 2020)

Counsel: For UNITED STATES OF AMERICA, Plaintiff - Appellee (13-50572, 13-50578, 13-50580, 14-50051): Jeffrey Michael Smith, Washington, DC; Daniel Earl Zipp, Assistant U.S. Attorney, San Diego, CA.

For BASAALY SAEED ***MOALIN***, AKA: Basal, AKA: Muse Shekhnor Roble, Defendant - Appellant (13-50572): Joshua L. Dratel, Law Offices of Joshua L. Dratel, P.C., New York, NY; Alexander A. Abdo, Knight First Amendment Institute at Columbia University, New York, NY; Patrick C. Toomey, American Civil Liberties Union Foundation, Washington, DC.

For BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, AMERICAN LIBRARY ASSOCIATION, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOM TO READ FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, NINTH CIRCUIT FEDERAL AND COMMUNITY DEFENDERS, and REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, Amicus Curiae (13-50572, 13-50578, 13-50580, 14-50051): Faiza Patel, Brennan Center for Justice, New York, NY.

For MOHAMED MOHAMED MOHAMUD, AKA: Mohamed Khadar, AKA: Sheikh Mohamed, Defendant - Appellant (13-50578): David **[*2]** James ***Zugman***, Attorney, Burcham & ***Zugman***, San Diego, CA.

For ISSA DOREH, AKA: Sheikh Issa, Defendant - Appellant (13-50580): Elizabeth Armena Missakian, Attorney, Law Office of Elizabeth A. Missakian, San Diego, CA.

For AHMED NASIR TAALIL MOHAMUD, Defendant - Appellant (14-50051): Benjamin Lee Coleman, Benjamin L. Coleman Law, PC, San Diego, CA.

Judges: Before: BERZON and NGUYEN, Circuit Judges, and ZOUHARY,[*] District Judge.

Opinion by: Zouhary

Opinion

The panel has unanimously voted to deny the petitions for rehearing. Judge Nguyen has voted to deny the petitions for rehearing en banc. Judge Berzon and Judge Zouhary recommend denial of the petitions for rehearing en banc. The full court has been advised of the petition for rehearing en banc, and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 40. The petitions for rehearing are denied; the petitions for rehearing en banc are rejected.

Zouhary, J., Statement:

I agree with the decision to deny the petitions for rehearing. I write separately to provide some context on the notice issue.

Section 3504

The government argues 18 U.S.C. § 3504, which allows a defendant to challenge evidence allegedly obtained through unlawful surveillance, provides the proper framework for Appellants **[*3]** to challenge the surveillance evidence in this case. The government points out that "the [P]anel did not cite or address" § 3504. There are two reasons for this. First, a defendant cannot use § 3504 to challenge surveillance if they have no notice of surveillance in the first place. *See, e.g., FBI v. Fazaga*, 595 U.S. 344, 356, 142 S. Ct. 1051, 212 L. Ed. 2d 172 (2022) ("[I]ndividuals affected by FISA surveillance are very often unaware of the surveillance unless it is revealed by the [g]overnment."). But here, Appellants received notice. *United States v.* ***Moalin***, 973 F.3d 977, 998 (9th Cir. 2020) ("After defendants were indicted, the government notified them and the district court that it intended to 'use or disclose' in 'proceedings in this case information obtained or derived from electronic surveillance conducted pursuant to the authority of [FISA].'") (citing 50 U.S.C. § 1806(c)). Second, our Opinion examined whether Appellants were entitled to notice *under the* Fourth Amendment -- not what Appellants *should have done* after receiving that notice (i.e., exercise their rights under § 3504). *See id.* at 999 (discussing notice obligations under *Dalia v. United States*, 441 U.S. 238, 99 S. Ct. 1682, 60 L. Ed. 2d 177 (1979) and 18 U.S.C. § 2518(8)(d)).

National Security

The government also contends that our conclusion on notice will deter cooperation between intelligence agencies and harm national security. There are two problems with this argument. The government assumes our holding **[*4]** requires *disclosure* of sensitive information. As detailed below, the Opinion does no such thing -- *notice* that surveillance took place is all that is required. *See* ***Moalin***, 973 F.3d at 1001 (noting that "notice is distinct from disclosure."). Further, as Appellants point out in their opposition,

[*] The Honorable Jack Zouhary, United States District Judge for the Northern District of Ohio, sitting by designation.

the government has been providing analogous notice under FISA for decades and there is no evidence of a deterrent effect or harm to national security.

Fourth Amendment Notice

Finally, the government challenges our discussion of notice under the Fourth Amendment, arguing this portion of the Opinion is "broad dicta" that runs contrary to congressional intent.

The government asserts that we improperly rely on FISA legislative history that concerned only notice requirements for the execution of search warrants, and that Congress deliberately omitted any notice requirements when the surveillance targets foreigners abroad. As to FISA's legislative history, the government misstates the quoted Senate Report. The Report did not deal with surveillance connected to a warrant. ***Moalin***, 973 F.3d at 1000. But even if the government were correct in its depiction of congressional intent, it makes no difference. This portion of the Opinion, which addressed arguments raised by Appellants, examined **[*5]** what is required by the Fourth Amendment, not FISA. And, more importantly, the Fourth Amendment's applicability is not conditioned on whether there is a warrant or any statutory protection. We state:

> This constitutional notice requirement applies to surveillance conducted under FISA and the [FISA Amendments Act], which codify the requirement. . . . Where statutory protections are lacking, the Fourth Amendment's reasonableness requirement takes on importance as a limit on executive power, and notice is necessary so that criminal defendants may challenge surveillance as inconsistent with that requirement.

Id. at 1000-01.

The government also ignores Appellants' status, arguing the panel "extend[ed] Fourth Amendment rights to cover the government's foreign intelligence activities overseas." At the time of the surveillance, each of the Appellants had either U.S. citizenship or lawful status. ***Moalin***, 973 F.3d at 985 n.2 ("***Moalin*** and Doreh are U.S. citizens, M. Mohamud has refugee status, and Nasir Mohamud has a visa."). Even if the surveillance initially targeted only Al-Shabaab members abroad, the Appellants, all lawfully residing in the U.S., became targets at some point. *See id.* at 999 ("For our purposes, the essential insight of Cavanagh is that even if the Fourth Amendment applies differently in the foreign intelligence **[*6]** context, it still *applies*, at least as U.S. persons are involved.") (citing *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1972)).

The government next argues "[t]he notice rule invented by the [P]anel in this case has no legal basis and has been rejected by at least three other courts." In support, the government cites a single appellate case, *United States v. Muhtorov*, 20 F.4th 558 (10th Cir. 2021). There, defendant, a lawful permanent resident, received government attention resulting from warrantless § 702 FISA surveillance targeting foreigners abroad. *Id.* at 581. The government used communications obtained through the warrantless surveillance to support further surveillance applications. *Id.* This led to a collection of incriminating statements and the FBI arresting defendant at an airport with cash and other incriminating items. *Id.* But unlike ***Moalin***, the government in that case "filed notice that it had used Section 702 to develop evidence against [him]." *Id.* at 590.

The government asserts that Muhtorov "rejected" a notice requirement. But the opinions don't conflict. Muhtorov concerned, in part, the government's discovery obligations and whether defendant was entitled to *disclosure of* the government's "novel surveillance techniques." 20 F.4th at 632. Our Opinion addressed notice -- not disclosure of techniques -- stating:

> We emphasize that notice is distinct **[*7]** from disclosure. Given the need for secrecy in the foreign intelligence context, the government is required only to inform the defendant that surveillance occurred and that the government intends to use information obtained or derived from it. . . . If the government avers that disclosure of information relating to the surveillance would harm national security, then the court can review the materials bearing on its legality *in camera* and *ex parte*.

Moalin, 973 F.3d at 1001. Additionally, defendant in Muhtorov sought disclosure of surveillance techniques under FISA and the Due Process Clause -- not the Fourth Amendment. 20 F.4th at 630-31.

Though our Fourth Amendment notice ruling may not have been "necessary to decide the case," there are critical reasons for making it. Executive Orders, like EO 12,333, remain outside the scope of FISA and the FAA, and contain no notice requirement. ***Moalin***, 973 F.3d at 999. Again, without any statutory protections, "the Fourth Amendment's reasonableness requirement takes on importance as a limit on executive power, and notice is necessary so that criminal defendants may challenge surveillance as inconsistent with that requirement." *Id.* at 1001. It is for these reasons, the panel struck a balance between the need for secrecy in national-security investigations and a defendant's right to challenge evidence. **[*8]**

End of Document

APPENDIX C: District Court's Order Denying Motion to Suppress

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 AMENDED ORDER DENYING MOTION FOR NEW TRIAL

The court issues this Amended Order Denying Motion for New Trial to correct a factual misstatement in its November 14, 2013 Order Denying Motion for New Trial ("Order"). (Ct. Dkt. 386). The court deletes the phrase "and the telephony metadata collected from the NSA program was either provided," (Ct. Dkt. 386 at p.7:15-16), and replaces it with "and the telephony metadata, collected pursuant to the FISA warrants and subpoenaed telephone toll records, was either provided." The Amended Order follows:

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

[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.

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 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 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

---

[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).

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.

---

[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).

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 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 pursuant to the FISA warrants and subpoenaed telephone toll records, 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

[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.

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 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.

---

[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."

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 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 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.

---

[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.

[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

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 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

---

and other relevant legal principles to this motion.

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 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.

---

[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).

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 18, 2013

Hon. Jeffrey T. Miller
United States District Judge

cc: All parties

APPENDIX D: Involved Law

U.S. Constitution

U.S. Const. Amend IV:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. Amend V:

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

U.S. Const. Amend VI:

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with

the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

Federal Statutes

18 U.S.C. § 956

18 U.S.C. § 1956

18 U.S.C. § 2332a

18 U.S.C. § 2339A

18 U.S.C. § 2339B

18 U.S.C. § 2339B

50 U.S.C. § 1861.

18 U.S. Code § 956 - Conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign country

U.S. Code Notes

(a)

(1) Whoever, within the jurisdiction of the United States, conspires with one or more other persons, regardless of where such other person or persons are located, to commit at any place outside the United States an act that would constitute the offense of murder, kidnapping, or maiming if committed in the special maritime and territorial jurisdiction of the United States shall, if any of the conspirators commits an act within the jurisdiction of the United States to effect any object of the conspiracy, be punished as provided in subsection (a)(2).

(2) The punishment for an offense under subsection (a)(1) of this section is—

(A) imprisonment for any term of years or for life if the offense is conspiracy to murder or kidnap; and

(B) imprisonment for not more than 35 years if the offense is conspiracy to maim.

(b) 96 Whoever, within the jurisdiction of the United States, conspires with one or more persons, regardless of where such other person or persons are located, to damage or destroy specific property situated within a foreign country and belonging to a foreign government or to any political subdivision thereof with which the United States is at peace, or any railroad, canal, bridge, airport, airfield, or other public utility, public conveyance, or public structure, or any religious, educational, or cultural property so situated, shall, if any of the conspirators commits an act within the jurisdiction of the United States to effect any object of the conspiracy, be imprisoned not more than 25 years.

(June 25, 1948, ch. 645, 62 Stat. 744; Pub. L. 103–322, title XXXIII, § 330016(1)(K), Sept. 13, 1994, 108 Stat. 2147; Pub. L. 104–132, title VII, § 704(a), Apr. 24, 1996, 110 Stat. 1294.)

18 U.S. Code § 1956 - Laundering of monetary instruments

U.S. Code | Notes | Authorities (CFR)

(a)

(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A)

(i) with the intent to promote the carrying on of specified unlawful activity; or

(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both. For purposes of this paragraph, a financial transaction shall be considered to be one involving the proceeds of specified unlawful activity if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement.

(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States—

(A) with the intent to promote the carrying on of specified unlawful activity; or

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than $500,000 or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for not more than twenty years, or both. For the purpose of the offense described in subparagraph (B), the defendant's knowledge may be established by proof that a law enforcement officer represented the matter specified in subparagraph (B) as true, and the defendant's subsequent statements or actions indicate that the defendant believed such representations to be true.

(3) Whoever, with the intent—

(A) to promote the carrying on of specified unlawful activity;

(B) to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or

(C) to avoid a transaction reporting requirement under State or Federal law,

conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, shall be fined under this title or imprisoned for not more than 20 years, or both. For purposes of this paragraph and paragraph (2), the term "represented" means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a Federal official authorized to investigate or prosecute violations of this section.

(b) PENALTIES.—

(1)In general.—Whoever conducts or attempts to conduct a transaction described in subsection (a)(1) or (a)(3), or section 1957, or a transportation, transmission, or transfer described in subsection (a)(2), is liable to the United States for a civil penalty of not more than the greater of—

(A)the value of the property, funds, or monetary instruments involved in the transaction; or

(B)$10,000.

(2)Jurisdiction over foreign persons.—For purposes of adjudicating an action filed or enforcing a penalty ordered under this section, the district courts shall have jurisdiction over any foreign person, including any financial institution authorized under the laws of a foreign country, against whom the action is brought, if service of process upon the foreign person is made under the Federal Rules of Civil Procedure or the laws of the country in which the foreign person is found, and—

(A)the foreign person commits an offense under subsection (a) involving a financial transaction that occurs in whole or in part in the United States;

(B)the foreign person converts, to his or her own use, property in which the United States has an ownership interest by virtue of the entry of an order of forfeiture by a court of the United States; or

(C)the foreign person is a financial institution that maintains a bank account at a financial institution in the United States.

(3)Court authority over assets.—
A court may issue a pretrial restraining order or take any other action necessary to ensure that any bank account or other property held by the defendant in the United States is available to satisfy a judgment under this section.

(4)Federal receiver.—

(A) In general.—
A court may appoint a Federal Receiver, in accordance with subparagraph (B) of this paragraph, to collect, marshal, and take custody, control, and possession of all assets of the defendant, wherever located, to satisfy a civil judgment under this subsection, a forfeiture judgment under section 981 or 982, or a criminal sentence under section 1957 or subsection (a) of this section, including an order of restitution to any victim of a specified unlawful activity.

(B) Appointment and authority.—A Federal Receiver described in subparagraph (A)—

(i)may be appointed upon application of a Federal prosecutor or a Federal or State regulator, by the court having jurisdiction over the

defendant in the case;

(ii) shall be an officer of the court, and the powers of the Federal Receiver shall include the powers set out in section 754 of title 28, United States Code; and

(iii) shall have standing equivalent to that of a Federal prosecutor for the purpose of submitting requests to obtain information regarding the assets of the defendant—

(I) from the Financial Crimes Enforcement Network of the Department of the Treasury; or

(II) from a foreign country pursuant to a mutual legal assistance treaty, multilateral agreement, or other arrangement for international law enforcement assistance, provided that such requests are in accordance with the policies and procedures of the Attorney General.

(c) As used in this section—

(1) the term "knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity" means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State, Federal, or foreign law, regardless of whether or not such activity is specified in paragraph (7);

(2) the term "conducts" includes initiating, concluding, or participating in initiating, or concluding a transaction;

(3) the term "transaction" includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected;

(4) the term "financial transaction" means (A) a transaction which in any way or degree affects interstate or foreign commerce (i) involving the movement of funds by wire or other means or (ii) involving one or more monetary instruments, or (iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree;

(5)the term "monetary instruments" means (i) coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, and money orders, or (ii) investment securities or negotiable instruments, in bearer form or otherwise in such form that title thereto passes upon delivery;

(6)the term "financial institution" includes—

(A)any financial institution, as defined in section 5312(a)(2) of title 31, United States Code, or the regulations promulgated thereunder; and

(B)any foreign bank, as defined in section 1 of the International Banking Act of 1978 (12 U.S.C. 3101);

(7)the term "specified unlawful activity" means—

(A)any act or activity constituting an offense listed in section 1961(1) of this title except an act which is indictable under subchapter II of chapter 53 of title 31;

(B)with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving—

(i)the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purposes of the Controlled Substances Act);

(ii)murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence (as defined in section 16);

(iii)fraud, or any scheme or attempt to defraud, by or against a foreign bank (as defined in paragraph 7 of section 1(b) of the International Banking Act of 1978));[1]

(iv)bribery of a public official, or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official;

(v)smuggling or export control violations involving—

(I)an item controlled on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. 2778); or

(II)an item controlled under regulations under the Export Administration Regulations (15 C.F.R. Parts 730–774);

(vi)an offense with respect to which the United States would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States; or

(vii) trafficking in persons, selling or buying of children, sexual exploitation of children, or transporting, recruiting or harboring a person, including a child, for commercial sex acts;

(C) any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848);

(D) an offense under section 32 (relating to the destruction of aircraft), section 37 (relating to violence at international airports), section 115 (relating to influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member), section 152 (relating to concealment of assets; false oaths and claims; bribery), section 175c (relating to the variola virus), section 215 (relating to commissions or gifts for procuring loans), section 351 (relating to congressional or Cabinet officer assassination), any of sections 500 through 503 (relating to certain counterfeiting offenses), section 513 (relating to securities of States and private entities), section 541 (relating to goods falsely classified), section 542 (relating to entry of goods by means of false statements), section 545 (relating to smuggling goods into the United States), section 549 (relating to removing goods from Customs custody), section 554 (relating to smuggling goods from the United States), section 555 (relating to border tunnels), section 641 (relating to public money, property, or records), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), section 657 (relating to lending, credit, and insurance institutions), section 658 (relating to property mortgaged or pledged to farm credit agencies), section 666 (relating to theft or bribery concerning programs receiving Federal funds), section 793, 794, or 798 (relating to espionage), section 831 (relating to prohibited transactions involving nuclear materials), section 844(f) or (i) (relating to destruction by explosives or fire of Government property or property affecting interstate or foreign commerce), section 875 (relating to interstate communications), section 922(l) (relating to the unlawful importation of firearms), section 924(n), 932, or 933 (relating to firearms trafficking), section 956 (relating to conspiracy to kill, kidnap, maim, or injure certain property in a foreign country), section 1005 (relating to fraudulent bank entries), 1006 [2] (relating to fraudulent Federal credit institution entries), 1007 [2] (relating to Federal Deposit Insurance transactions), 1014 [2] (relating to fraudulent loan or credit applications), section 1030 (relating to computer fraud and abuse), 1032 [2] (relating to concealment of assets from conservator, receiver, or liquidating agent of financial institution), section 1111 (relating to murder), section 1114 (relating to murder of United States law enforcement officials), section 1116 (relating to murder of foreign officials, official guests, or internationally protected persons), section 1201 (relating to kidnaping), section 1203 (relating to hostage taking), section 1361 (relating to willful injury of Government property), section 1363 (relating to destruction of property within the special maritime and territorial jurisdiction), section 1708 (theft

from the mail), section 1751 (relating to Presidential assassination), section 2113 or 2114 (relating to bank and postal robbery and theft), section 2252A (relating to child pornography) where the child pornography contains a visual depiction of an actual minor engaging in sexually explicit conduct, section 2260 (production of certain child pornography for importation into the United States), section 2280 (relating to violence against maritime navigation), section 2281 (relating to violence against maritime fixed platforms), section 2319 (relating to copyright infringement), section 2320 (relating to trafficking in counterfeit goods and services), section 2332 (relating to terrorist acts abroad against United States nationals), section 2332a (relating to use of weapons of mass destruction), section 2332b (relating to international terrorist acts transcending national boundaries), section 2332g (relating to missile systems designed to destroy aircraft), section 2332h (relating to radiological dispersal devices), section 2339A or 2339B (relating to providing material support to terrorists), section 2339C (relating to financing of terrorism), or section 2339D (relating to receiving military-type training from a foreign terrorist organization) of this title, section 46502 of title 49, United States Code, a felony violation of the Chemical Diversion and Trafficking Act of 1988 (relating to precursor and essential chemicals), section 590 of the Tariff Act of 1930 (19 U.S.C. 1590) (relating to aviation smuggling), section 422 of the Controlled Substances Act (relating to transportation of drug paraphernalia), section 38(c) (relating to criminal violations) of the Arms Export Control Act, section 11 [3] (relating to violations) of the Export Administration Act of 1979, section 206 (relating to penalties) of the International Emergency Economic Powers Act, section 16 (relating to offenses and punishment) of the Trading with the Enemy Act, any felony violation of section 15 of the Food and Nutrition Act of 2008 (relating to supplemental nutrition assistance program benefits fraud) involving a quantity of benefits having a value of not less than $5,000, any violation of section 543(a)(1) of the Housing Act of 1949 (relating to equity skimming), any felony violation of the Foreign Agents Registration Act of 1938, any felony violation of the Foreign Corrupt Practices Act, section 92 of the Atomic Energy Act of 1954 (42 U.S.C. 2122) (relating to prohibitions governing atomic weapons), or section 104(a) of the North Korea Sanctions Enforcement Act of 2016 [3] (relating to prohibited activities with respect to North Korea);

ENVIRONMENTAL CRIMES

(E) a felony violation of the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), the Ocean Dumping Act (33 U.S.C. 1401 et seq.), the Act to Prevent Pollution from Ships (33 U.S.C. 1901 et seq.), the Safe Drinking Water Act (42 U.S.C. 300f et seq.), or the Resources Conservation and Recovery Act (42 U.S.C. 6901 et seq.);

(F) any act or activity constituting an offense involving a Federal health care offense; or

(G) any act that is a criminal violation of subparagraph (A), (B), (C), (D), (E), or (F) of paragraph (1) of section 9(a) of the Endangered Species Act of 1973 (16 U.S.C. 1538(a)(1)), section 2203 of the African Elephant Conservation Act (16 U.S.C. 4223), or section 7(a) of the Rhinoceros and Tiger Conservation Act of 1994 (16 U.S.C. 5305a(a)), if the endangered or threatened species of fish or wildlife, products, items, or substances involved in the violation and relevant conduct, as applicable, have a total value of more than $10,000;

(8) the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States; and

(9) the term "proceeds" means any property derived from or obtained or retained, directly or indirectly, through some form of unlawful activity, including the gross receipts of such activity.

(d) Nothing in this section shall supersede any provision of Federal, State, or other law imposing criminal penalties or affording civil remedies in addition to those provided for in this section.

(e) Violations of this section may be investigated by such components of the Department of Justice as the Attorney General may direct, and by such components of the Department of the Treasury as the Secretary of the Treasury may direct, as appropriate, and, with respect to offenses over which the Department of Homeland Security has jurisdiction, by such components of the Department of Homeland Security as the Secretary of Homeland Security may direct, and, with respect to offenses over which the United States Postal Service has jurisdiction, by the Postal Service. Such authority of the Secretary of the Treasury, the Secretary of Homeland Security, and the Postal Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury, the Secretary of Homeland Security, the Postal Service, and the Attorney General. Violations of this section involving offenses described in paragraph (c)(7)(E) may be investigated by such components of the Department of Justice as the Attorney General may direct, and the National Enforcement Investigations Center of the Environmental Protection Agency.

(f) There is extraterritorial jurisdiction over the conduct prohibited by this section if—

(1) the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and

(2) the transaction or series of related transactions involves funds or monetary instruments of a value exceeding $10,000.

(g)Notice of Conviction of Financial Institutions.—
If any financial institution or any officer, director, or employee of any financial institution has been found guilty of an offense under this section, section 1957 or 1960 of this title, or section 5322 or 5324 of title 31, the Attorney General shall provide written notice of such fact to the appropriate regulatory agency for the financial institution.

(h) Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

(i)Venue.—

(1) Except as provided in paragraph (2), a prosecution for an offense under this section or section 1957 may be brought in—

(A)any district in which the financial or monetary transaction is conducted; or

(B)any district where a prosecution for the underlying specified unlawful activity could be brought, if the defendant participated in the transfer of the proceeds of the specified unlawful activity from that district to the district where the financial or monetary transaction is conducted.

(2)A prosecution for an attempt or conspiracy offense under this section or section 1957 may be brought in the district where venue would lie for the completed offense under paragraph (1), or in any other district where an act in furtherance of the attempt or conspiracy took place.

(3) For purposes of this section, a transfer of funds from 1 place to another, by wire or any other means, shall constitute a single, continuing transaction. Any person who conducts (as that term is defined in subsection (c)(2)) any portion of the transaction may be charged in any district in which the transaction takes place.

(j)Seven-year Limitation.—
Notwithstanding section 3282, no person shall be prosecuted, tried, or punished for a violation of this section or section 1957 if the specified unlawful activity constituting the violation is the activity defined in subsection (c)(7)(B) of this section, unless the indictment is found or the information is instituted not later than 7 years after the date on which the offense was committed.

(Added Pub. L. 99–570, title I, § 1352(a), Oct. 27, 1986, 100 Stat. 3207–18; amended Pub. L. 100–690, title VI, §§ 6183, 6465, 6466, 6469(a)(1), 6471(a), (b), title VII, § 7031, Nov. 18, 1988, 102 Stat. 4354, 4375, 4377, 4378, 4398; Pub. L. 101–647, title I, §§ 105–108, title XII, § 1205(j), title XIV, §§ 1402, 1404, title XXV, § 2506, title XXXV, § 3557, Nov. 29, 1990, 104

Stat. 4791, 4792, 4831, 4835, 4862, 4927; Pub. L. 102–550, title XV, §§ 1504(c), 1524, 1526(a), 1527(a), 1530, 1531, 1534, 1536, Oct. 28, 1992, 106 Stat. 4055, 4064–4067; Pub. L. 103–322, title XXXII, § 320104(b), title XXXIII, §§ 330008(2), 330011(*l*), 330012, 330019, 330021(1), Sept. 13, 1994, 108 Stat. 2111, 2142, 2145, 2146, 2149, 2150; Pub. L. 103–325, title IV, §§ 411(c)(2)(E), 413(c)(1), (d), Sept. 23, 1994, 108 Stat. 2253–2255; Pub. L. 104–132, title VII, § 726, Apr. 24, 1996, 110 Stat. 1301; Pub. L. 104–191, title II, § 246, Aug. 21, 1996, 110 Stat. 2018; Pub. L. 104–294, title VI, §§ 601(f)(6), 604(b)(38), Oct. 11, 1996, 110 Stat. 3499, 3509; Pub. L. 106–569, title VII, § 709(a), Dec. 27, 2000, 114 Stat. 3018; Pub. L. 107–56, title III, §§ 315, 317, 318, 376, title VIII, § 805(b), title X, § 1004, Oct. 26, 2001, 115 Stat. 308, 310, 311, 342, 378, 392; Pub. L. 107–273, div. B, title IV, §§ 4002(a)(11), (b)(5), (c)(2), 4005(d)(1), (e), Nov. 2, 2002, 116 Stat. 1807, 1809, 1812, 1813; Pub. L. 108–458, title VI, § 6909, Dec. 17, 2004, 118 Stat. 3774; Pub. L. 109–164, title I, § 103(b), Jan. 10, 2006, 119 Stat. 3563; Pub. L. 109–177, title III, § 311(c), title IV, §§ 403(b), (c)(1), 405, 406(a)(2), 409, Mar. 9, 2006, 120 Stat. 242–244, 246; Pub. L. 110–234, title IV, §§ 4002(b)(1)(B), (D), (2)(M), 4115(c)(1)(A)(i), (B)(ii), May 22, 2008, 122 Stat. 1096, 1097, 1109; Pub. L. 110–246, § 4(a), title IV, §§ 4002(b)(1)(B), (D), (2)(M), 4115(c)(1)(A)(i), (B)(ii), June 18, 2008, 122 Stat. 1664, 1857, 1858, 1870; Pub. L. 110–358, title II, § 202, Oct. 8, 2008, 122 Stat. 4003; Pub. L. 111–21, § 2(f)(1), May 20, 2009, 123 Stat. 1618; Pub. L. 112–127, § 6, June 5, 2012, 126 Stat. 371; Pub. L. 114–122, title I, § 105(c), Feb. 18, 2016, 130 Stat. 101; Pub. L. 114–231, title V, § 502, Oct. 7, 2016, 130 Stat. 956; Pub. L. 117–159, div. A, title II, § 12004(a)(4), June 25, 2022, 136 Stat. 1328; Pub. L. 117–263, div. E, title LIX, § 5904(a), Dec. 23, 2022, 136 Stat. 3441.)

18 U.S. Code § 2332a - Use of weapons of mass destruction

U.S. Code Notes

(a) Offense Against a National of the United States or Within the United States.—
A person who, without lawful authority, uses, threatens, or attempts or conspires to use, a weapon of mass destruction—

(1) against a national of the United States while such national is outside of the United States;

(2) against any person or property within the United States, and

(A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense;

(B) such property is used in interstate or foreign commerce or in an activity that affects interstate or foreign commerce;

(C) any perpetrator travels in or causes another to travel in interstate or foreign commerce in furtherance of the offense; or

(D) the offense, or the results of the offense, affect interstate or foreign commerce, or, in the case of a threat, attempt, or conspiracy, would have affected interstate or foreign commerce;

(3) against any property that is owned, leased or used by the United States or by any department or agency of the United States, whether the property is within or outside of the United States; or

(4) against any property within the United States that is owned, leased, or used by a foreign government,

shall be imprisoned for any term of years or for life, and if death results, shall be punished by death or imprisoned for any term of years or for life.

(b) Offense by National of the United States Outside of the United States.—
Any national of the United States who, without lawful authority, uses, or threatens, attempts, or conspires to use, a weapon of mass destruction outside of the United

States shall be imprisoned for any term of years or for life, and if death results, shall be punished by death, or by imprisonment for any term of years or for life.

(c) Definitions.—For purposes of this section—

(1) the term "national of the United States" has the meaning given in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22));

(2) the term "weapon of mass destruction" means—

(A) any destructive device as defined in section 921 of this title;

(B) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;

(C) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of this title); or

(D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life; and

(3) the term "property" includes all real and personal property.

(Added Pub. L. 103–322, title VI, § 60023(a), Sept. 13, 1994, 108 Stat. 1980; amended Pub. L. 104–132, title V, § 511(c), title VII, § 725, Apr. 24, 1996, 110 Stat. 1284, 1300; Pub. L. 104–294, title VI, § 605(m), Oct. 11, 1996, 110 Stat. 3510; Pub. L. 105–277, div. I, title II, § 201(b)(1), Oct. 21, 1998, 112 Stat. 2681–871; Pub. L. 107–188, title II, § 231(d), June 12, 2002, 116 Stat. 661; Pub. L. 108–458, title VI, § 6802(a), (b), Dec. 17, 2004, 118 Stat. 3766, 3767.)

18 U.S. Code § 2339B - Providing material support or resources to designated foreign terrorist organizations

(a) Prohibited Activities.—

(1) Unlawful conduct.—
Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989).

(2) Financial institutions.—Except as authorized by the Secretary, any financial institution that becomes aware that it has possession of, or control over, any funds in which a foreign terrorist organization, or its agent, has an interest, shall—

(A) retain possession of, or maintain control over, such funds; and

(B) report to the Secretary the existence of such funds in accordance with regulations issued by the Secretary.

(b) Civil Penalty.—Any financial institution that knowingly fails to comply with subsection (a)(2) shall be subject to a civil penalty in an amount that is the greater of—

(A) $50,000 per violation; or

(B) twice the amount of which the financial institution was required under subsection (a)(2) to retain possession or control.

(c) Injunction.—
Whenever it appears to the Secretary or the Attorney General that any person is engaged in, or is about to engage in, any act that constitutes, or would constitute, a violation of this section, the Attorney General may initiate civil action in a district court of the United States to enjoin such violation.

(d) Extraterritorial Jurisdiction.—

(1) In general.— There is jurisdiction over an offense under subsection (a) if—

(A) an offender is a national of the United States (as defined in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22))) or an alien lawfully admitted for permanent residence in the United States (as defined in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(20)));

(B) an offender is a stateless person whose habitual residence is in the United States;

(C) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States;

(D) the offense occurs in whole or in part within the United States;

(E) the offense occurs in or affects interstate or foreign commerce; or

(F) an offender aids or abets any person over whom jurisdiction exists under this paragraph in committing an offense under subsection (a) or conspires with any person over whom jurisdiction exists under this paragraph to commit an offense under subsection (a).

(2) Extraterritorial jurisdiction.—
There is extraterritorial Federal jurisdiction over an offense under this section.

(e) Investigations.—

(1) In general.—
The Attorney General shall conduct any investigation of a possible violation of this section, or of any license, order, or regulation issued pursuant to this section.

(2) Coordination with the department of the treasury.— The Attorney General shall work in coordination with the Secretary in investigations relating to—

(A) the compliance or noncompliance by a financial institution with the requirements of subsection (a)(2); and

(B) civil penalty proceedings authorized under subsection (b).

(3) Referral.—
Any evidence of a criminal violation of this section arising in the course of an investigation by the Secretary or any other Federal agency shall be referred immediately to the Attorney General for further investigation. The Attorney General shall timely notify the Secretary of any action taken on referrals from the Secretary, and may refer investigations to the Secretary for remedial licensing or civil penalty action.

(f) Classified Information in Civil Proceedings Brought by the United States.—

(1) Discovery of classified information by defendants.—

(A) Request by united states.—In any civil proceeding under this section, upon request made ex parte and in writing by the United States, a court, upon a sufficient showing, may authorize the United States to—

(i) redact specified items of classified information from documents to be introduced into evidence or made available to the defendant through discovery under the Federal Rules of Civil Procedure;

(ii) substitute a summary of the information for such classified documents; or

(iii) substitute a statement admitting relevant facts that the classified information would tend to prove.

(B) Order granting request.—
If the court enters an order granting a request under this paragraph, the entire text of the documents to which the request relates shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

(C) Denial of request.—
If the court enters an order denying a request of the United States under this paragraph, the United States may take an immediate, interlocutory appeal in accordance with paragraph (5). For purposes of such an appeal, the entire text of the documents to which the request relates, together with any transcripts of arguments made ex parte to the court in connection therewith, shall be maintained under seal and delivered to the appellate court.

(2)Introduction of classified information; precautions by court.—

(A) Exhibits.—To prevent unnecessary or inadvertent disclosure of classified information in a civil proceeding brought by the United States under this section, the United States may petition the court ex parte to admit, in lieu of classified writings, recordings, or photographs, one or more of the following:

(i) Copies of items from which classified information has been redacted.

(ii) Stipulations admitting relevant facts that specific classified information would tend to prove.

(iii)A declassified summary of the specific classified information.

(B) Determination by court.—
The court shall grant a request under this paragraph if the court finds that the redacted item, stipulation, or summary is sufficient to allow the defendant to prepare a defense.

(3)Taking of trial testimony.—

(A) Objection.—
During the examination of a witness in any civil proceeding brought by the United States under this subsection, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible.

(B) Action by court.—In determining whether a response is admissible, the court shall take precautions to guard against the compromise of any classified information, including—

(i)permitting the United States to provide the court, ex parte, with a proffer of the witness's response to the question or line of inquiry; and

(ii)requiring the defendant to provide the court with a proffer of the nature of the information that the defendant seeks to elicit.

(C) Obligation of defendant.—
In any civil proceeding under this section, it shall be the defendant's obligation to establish the relevance and materiality of any classified information sought to be introduced.

(4)Appeal.—
If the court enters an order denying a request of the United States under this subsection, the United States may take an immediate interlocutory appeal in

accordance with paragraph (5).

(5) **Interlocutory appeal.—**

(A) Subject of appeal.—An interlocutory appeal by the United States shall lie to a court of appeals from a decision or order of a district court—

(i) authorizing the disclosure of classified information;

(ii) imposing sanctions for nondisclosure of classified information; or

(iii) refusing a protective order sought by the United States to prevent the disclosure of classified information.

(B) Expedited consideration.—

(i) In general.—
An appeal taken pursuant to this paragraph, either before or during trial, shall be expedited by the court of appeals.

(ii) Appeals prior to trial.—
If an appeal is of an order made prior to trial, an appeal shall be taken not later than 14 days after the decision or order appealed from, and the trial shall not commence until the appeal is resolved.

(iii) Appeals during trial.—If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved, and the court of appeals—

(I) shall hear argument on such appeal not later than 4 days after the adjournment of the trial, excluding intermediate weekends and holidays;

(II) may dispense with written briefs other than the supporting materials previously submitted to the trial court;

(III) shall render its decision not later than 4 days after argument on appeal, excluding intermediate weekends and holidays; and

(IV) may dispense with the issuance of a written opinion in rendering its decision.

(C) Effect of ruling.—
An interlocutory appeal and decision shall not affect the right of the defendant, in a subsequent appeal from a final judgment, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.

(6) **Construction.—**

Nothing in this subsection shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information, including the invocation of the military and State secrets privilege.

(g) Definitions.—As used in this section—

(1) the term "classified information" has the meaning given that term in section 1(a) of the Classified Information Procedures Act (18 U.S.C. App.);

(2) the term "financial institution" has the same meaning as in section 5312(a)(2) of title 31, United States Code;

(3) the term "funds" includes coin or currency of the United States or any other country, traveler's checks, personal checks, bank checks, money orders, stocks, bonds, debentures, drafts, letters of credit, any other negotiable instrument, and any electronic representation of any of the foregoing;

(4) the term "material support or resources" has the same meaning given that term in section 2339A (including the definitions of "training" and "expert advice or assistance" in that section);

(5) the term "Secretary" means the Secretary of the Treasury; and

(6) the term "terrorist organization" means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act.

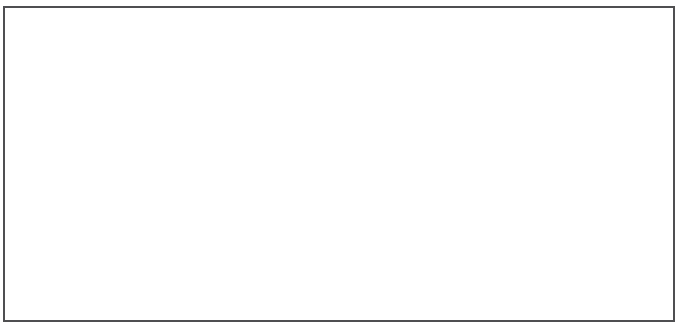
(h) Provision of Personnel.—
No person may be prosecuted under this section in connection with the term "personnel" unless that person has knowingly provided, attempted to provide, or conspired to provide a foreign terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization. Individuals who act entirely independently of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization's direction and control.

(i) Rule of Construction.—
Nothing 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.

(j) Exception.—

No person may be prosecuted under this section in connection with the term "personnel", "training", or "expert advice or assistance" if the provision of that material support or resources to a foreign terrorist organization was approved by the Secretary of State with the concurrence of the Attorney General. The Secretary of State may not approve the provision of any material support that may be used to carry out terrorist activity (as defined in section 212(a)(3)(B)(iii) of the Immigration and Nationality Act).

(Added Pub. L. 104–132, title III, § 303(a), Apr. 24, 1996, 110 Stat. 1250; amended Pub. L. 107–56, title VIII, § 810(d), Oct. 26, 2001, 115 Stat. 380; Pub. L. 108–458, title VI, § 6603(c)–(f), Dec. 17, 2004, 118 Stat. 3762, 3763; Pub. L. 111–16, § 3(6)–(8), May 7, 2009, 123 Stat. 1608; Pub. L. 114–23, title VII, § 704, June 2, 2015, 129 Stat. 300.)



18 U.S. Code § 2339A - Providing material support to terrorists

U.S. Code Notes

(a) Offense.—
Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of section 32, 37, 81, 175, 229, 351, 831, 842(m) or (n), 844(f) or (i), 930(c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, or 2442 of this title, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), section 46502 or 60123(b) of title 49, or any offense listed in section 2332b(g)(5)(B) (except for sections 2339A and 2339B) or in preparation for, or in carrying out, the concealment of an escape from the commission of any such violation, or attempts or conspires to do such an act, shall be fined under this title, imprisoned not more than 15 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law.

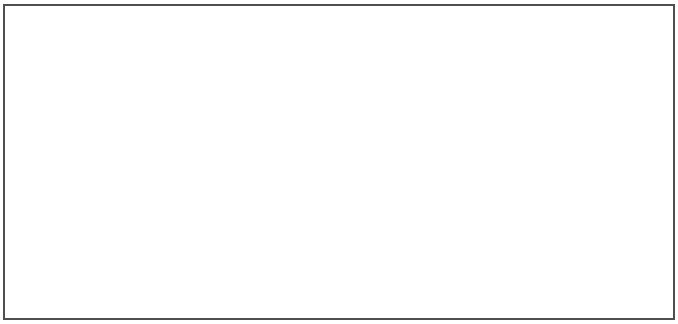
(b) Definitions.—As used in this section—

(1) the term "material support or resources" means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials;

(2) the term "training" means instruction or teaching designed to impart a specific skill, as opposed to general knowledge; and

(3) the term "expert advice or assistance" means advice or assistance derived from scientific, technical or other specialized knowledge.

(Added Pub. L. 103–322, title XII, § 120005(a), Sept. 13, 1994, 108 Stat. 2022; amended Pub. L. 104–132, title III, § 323, Apr. 24, 1996, 110 Stat. 1255; Pub. L. 104–294, title VI, §§ 601(b)(2), (s)(2), (3), 604(b)(5), Oct. 11, 1996, 110 Stat. 3498, 3502, 3506; Pub. L. 107–56, title VIII, §§ 805(a), 810(c), 811(f), Oct. 26, 2001, 115 Stat. 377, 380, 381; Pub. L. 107–197, title III, § 301(c), June 25, 2002, 116 Stat. 728; Pub. L. 107–273, div. B, title IV, § 4002(a)(7), (c)(1), (e)(11), Nov. 2, 2002, 116 Stat. 1807, 1808, 1811; Pub. L. 108–458, title VI, § 6603(a)(2), (b), Dec. 17, 2004, 118 Stat. 3762; Pub. L. 109–177, title I, § 110(b)(3)(B), Mar. 9, 2006, 120 Stat. 208; Pub. L. 111–122, § 3(d), Dec. 22, 2009, 123 Stat. 3481.)



50 U.S. Code § 1861 - Definitions

U.S. Code Notes

As used in this subchapter:

(1) The terms "foreign power", "agent of a foreign power", "foreign intelligence information", "international terrorism", and "Attorney General" shall have the same meanings as in section 1801 of this title.

(2) The term "common carrier" means any person or entity transporting people or property by land, rail, water, or air for compensation.

(3) The term "physical storage facility" means any business or entity that provides space for the storage of goods or materials, or services related to the storage of goods or materials, to the public or any segment thereof.

(4) The term "public accommodation facility" means any inn, hotel, motel, or other establishment that provides lodging to transient guests.

(5) The term "vehicle rental facility" means any person or entity that provides vehicles for rent, lease, loan, or other similar use to the public or any segment thereof.

(Pub. L. 95–511, title V, § 501, as added Pub. L. 107–56, title II, § 215, Oct. 26, 2001, 115 Stat. 287; amended Pub. L. 107–108, title III, § 314(a)(6), Dec. 28, 2001, 115 Stat. 1402; Pub. L. 109–177, title I, §§ 102(b)(1), 106(a)–(e), (f)(2), (g), Mar. 9, 2006, 120 Stat. 195–198; Pub. L. 109–178, §§ 3, 4(a), Mar. 9, 2006, 120 Stat. 278, 280; Pub. L. 111–118, div. B, § 1004(a), Dec. 19, 2009, 123 Stat. 3470; Pub. L. 111–141, § 1(a), Feb. 27, 2010, 124 Stat. 37; Pub. L. 112–3, § 2(a), Feb. 25, 2011, 125 Stat. 5; Pub. L. 112–14, § 2(a), May 26, 2011, 125 Stat. 216; Pub. L. 114–23, title I, §§ 101–107, title VII, § 705(a), (c), June 2, 2015, 129 Stat. 269–273, 300; Pub. L. 115–118, title II, § 205(b)(6), Jan. 19, 2018, 132 Stat. 22; Pub. L. 116–69, div. B, title VII, § 1703(a), Nov. 21, 2019, 133 Stat. 1143.)