FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. BASAALY SAEED MOALIN, AKA Basal, AKA Muse Shekhnor Roble, *Defendant-Appellant.*	No. 13-50572 D.C. No. 3:10-cr-04246-JM-1
UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. MOHAMED MOHAMED MOHAMUD, AKA Mohamed Khadar, AKA Sheikh Mohamed, *Defendant-Appellant.*	No. 13-50578 D.C. No. 3:10-cr-04246-JM-2
UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. ISSA DOREH, AKA Sheikh Issa, *Defendant-Appellant*.	No. 13-50580 D.C. No. 3:10-cr-04246-JM-3

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. AHMED NASIR TAALIL MOHAMUD, *Defendant-Appellant.*	No. 14-50051 D.C. No. 3:10-cr-04246-JM-4 OPINION

Appeal from the United States District Court
for the Southern District of California
Jeffrey T. Miller, District Judge, Presiding

Argued and Submitted November 10, 2016
Pasadena, California

Filed September 2, 2020

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

Opinion by Judge Berzon

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

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

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

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 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 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, 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.

OPINION

BERZON, Circuit Judge:

INTRODUCTION

Four members of the Somali diaspora appeal from their 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 these issues and several others raised by the defendants, we affirm the convictions in all respects.

BACKGROUND[1]

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

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

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 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 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 18 U.S.C. § 2339B(a)(1); and conspiracy to launder monetary instruments, 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

[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.

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 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 "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," "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 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 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.

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

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 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 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 disclosures, then-FBI Deputy Director Sean Joyce described a post-9/11 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 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 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 from [redacted]*, No. BR 13-80, 2013 WL 5460137, at *1 (FISA Ct. Apr. 25, 2013). These orders required major 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 WL 5741573, at *1 (FISA Ct. Aug. 29, 2013) ("*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." *Id.* at *10. These records included

[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).

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. *Id.* 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 id.* 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 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 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 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 (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 (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 they voluntarily convey to the telephone company. *Id.* at 742–43. *Smith* relied on *United States v. Miller*, 425 U.S. 435 (1976), which had held that defendants had no legitimate expectation of privacy in their bank 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 (2018) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (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 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, 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 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 (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 Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." *In re Application II*, 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 (D.C. Cir. 2015). According to the NSA's former general counsel Stewart Baker, "[m]etadata absolutely tells 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 (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, "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 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 (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." 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 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 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 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 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 (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

[6] Defendants, relying on *Alderman v. United States*, 394 U.S. 165 (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.

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 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 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 . . . 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]

[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.

[8] Unlike *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), this case is a criminal prosecution, so there is no Article III standing issue here.

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 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.

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

§ 1861(b)(2)(A) (2006) (emphasis added).[10] Defendants argue that the metadata 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 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 (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 interpretation of the word "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

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

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, "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 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 associated with a foreign terrorist—were clearly relevant to a counterterrorism 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

[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

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 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.

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 in

---

suppression would not be warranted were we to decide that the metadata program violated the Fourth Amendment. *See supra* p. 23.

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 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 (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 (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 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

[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).

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).

Contrary 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 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 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.

[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 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 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 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 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.

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 (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

[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).

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 substitute for advance notice." *Dalia v. United States*, 441 U.S. 238, 248 (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 (1977).

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 (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 did not address the Fourth Amendment's notice requirement, 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

[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 (2013)).

the Fourth Amendment's requirements, whatever the parameters 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 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 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*

[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).

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 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 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. 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. *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 (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 (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 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 (1985).[17] We review de novo whether a *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

[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).

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 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.

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 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 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 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, 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.

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

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 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. 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*

[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.

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 request to compel immunity implicates "important separation 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

[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).

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 the government had named Shidane as "uncharged co-conspirator #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 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 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 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 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 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 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 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 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 the conspiracy. *See id.* §§ 2339A, 2339B(a)(1); *Whitfield v. United States*, 543 U.S. 209, 219 (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 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 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 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 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, 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

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

an acquaintance: "[T]he gentlemen [sic] called me this morning. . . . [W]e had a heated debate. He said . . . [']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 to." Nine minutes 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 Mohamed told Moalin: "It was sent in installments. That is what they did." Later on April 25, 2008, Moalin called Abdirizak and 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. 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 talking about something else now, about the youngsters; . . . there were two cartons that I allocated for them. . . ." Doreh responded throughout 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.* § 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.**