Linda Lye (CA SBN 215584)
llye@aclunc.org
Matthew T. Cagle (CA SBN 286101)
mcagle@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 621-2493
Fax: (415) 255-8437

Patrick Toomey (admitted *pro hac vice*)
ptoomey@aclu.org
Anna Diakun (admitted *pro hac vice*)
adiakun@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO-OAKLAND DIVISION

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA; AMERICAN CIVIL LIBERTIES UNION; AMERICNA CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. DEPARTMENT OF JUSTICE, Defendant.	Case No. 4:17-cv-03571 JSW SECOND DECLARATION OF MATTHEW CAGLE

I, Matthew Cagle, declare as follows:

1. My name is Matthew Cagle. I am counsel for Plaintiffs in the above-referenced action. The information in this declaration is based upon my personal knowledge and if called upon to testify, I could and would competently testify thereto.

2. I submit this declaration in support of Plaintiffs' Supplemental Brief Regarding Recent Authority.

3. I am an attorney with the ACLU Foundation of Northern California. In my capacity as an attorney, I work on issues pertaining to, among other things, privacy, technology, and electronic surveillance.

4. Attached as Exhibit 1 is a true and correct copy of the relevant pages from the Cunningham Decl., *ACLU-NC v. DOJ*, No. 12-cv-04008-MEJ (N.D. Cal. June 6, 2013), ECF No. 23-2, which I obtained from the files maintained by my office. This matter was litigated by my office and pleadings from that case were kept in the ordinary course of business.

5. Attached as Exhibit 2 is a true and correct copy of the relevant pages from Answering Br. of the United States, *United States v. Moalin*, No. 13-50572, at 39-47 (9th Cir. Apr. 15, 2016), ECF No. 34-1, which I obtained from Pacer.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed this 9th day of February in San Francisco, California.

/s/Matthew Cagle

Matthew Cagle

Filer's Attestation

I, Linda Lye, am the ECF user whose identification and password are being used to file this SECOND DECLARATION OF MATTHEW CAGLE. Pursuant to Local Rule 5-1(i)(3), I hereby attest that concurrence in the electronic filing of this document has been obtained from the other signatory.

Dated: February 9, 2018 By /s/ *Linda Lye*
Linda Lye

EXHIBIT 1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA; SAN FRANCISCO BAY GUARDIAN, Plaintiffs, v. U.S. DEPARTMENT OF JUSTICE, Defendant.	Case No. 12-cv-4008-MEJ DECLARATION OF JOHN E. CUNNINGHAM III

I, John E. Cunningham III, declare the following to be a true and correct statement of facts:

1. I am a Trial Attorney in the Freedom of Information Act ("FOIA")/Privacy Act ("PA") Unit of the Office of Enforcement Operations in the Criminal Division of the United States Department of Justice (the "Criminal Division"). I have held this position since November of 2011. Prior to that time, I was employed as a Trial Attorney in the Criminal Division's Fraud Section since 1998.

2. The FOIA/PA Unit is responsible for processing FOIA/PA requests seeking information from the Criminal Division. FOIA/PA Unit staff determine whether the Criminal Division maintains records responsive to access requests, and if so, whether they can be released in accordance with the FOIA/PA. In processing such requests, the FOIA/PA Unit consults with personnel in the other Sections of the Criminal Division, and when appropriate, with other components within the Department of Justice ("DOJ"), as well as with other Executive Branch agencies.

3. In my capacity as a Trial Attorney, and in conjunction with the Acting Chief of the FOIA/PA Unit, I assist in supervising the handling of FOIA and PA requests processed by the FOIA/PA Unit. I am responsible for providing litigation support and assistance to Assistant

United States Attorneys and Civil Division Trial Attorneys who represent the DOJ in lawsuits brought under FOIA, 5 U.S.C. § 552, and the PA, 5 U.S.C. § 552a, stemming from requests for Criminal Division records.

4. In providing such support and assistance, I review processing files compiled in responding to FOIA/PA requests received by the Criminal Division to determine whether searches for records were properly conducted and whether decisions to withhold or release Criminal Division records were in accordance with the FOIA and PA, as well as DOJ FOIA and PA regulations at 28 C.F.R. § 16.1 et seq. If searches are incomplete and/or records have not been processed, I oversee the completion of any pending searches of Criminal Division documents by FOIA/PA staff members. I consult with the Acting Chief of the FOIA/PA Unit, the Supervisory FOIA Specialist, the other FOIA Specialists, and other members of the Unit about the Criminal Division's searches and processing of FOIA/PA requests.

5. Due to the nature of my official duties, I am familiar with, and was personally involved in, the processing of the FOIA request submitted by plaintiffs the American Civil Liberties Union of Northern California ("ACLU-NC") and San Francisco Bay Guardian ("Bay Guardian") that is at issue in this litigation. I make the statements herein on the basis of personal knowledge, as well as on information acquired by me in the course of performing my official duties in the FOIA/PA Unit.

6. I submit this declaration in support of DOJ's motion for partial summary judgment and to describe the information being withheld from the responsive records and the exemptions the Criminal Division has applied, in accordance with *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973).

Plaintiffs' FOIA Request and Referral to the Criminal Division

7. By letter dated April 13, 2012, Nicole A. Ozer, on behalf of the ACLU-NC and the Bay Guardian, submitted a FOIA request (the "FOIA Request") addressed to the United States Attorney for the Northern District of California ("USACAN") and the Office of Public Affairs of the United States Department of Justice seeking:

1) All requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008.

2) Any template applications or orders that have been utilized by United States Attorneys in the Northern District to seek or acquire location information since January 1, 2008.

3) Any documents since January 1, 2008, related to the use or policies of utilizing any location tracking technology, including but not limited to cell-site simulators or digital analyzers such as devices known as Stingray, Triggerfish, AmberJack, KingFish or Loggerhead.

4) Any records related to the Supreme Court's holding in *United States v. Jones*, excluding pleadings or court opinions filed in the matter in the Supreme Court or courts below.

A true and correct copy of the ACLU-NC's FOIA Request is attached as Exhibit 1. I am also familiar with the January 3, 2013, stipulation entered into by the parties in this matter. *See* ECF No. 17.

8. By way of e-mail dated February 27, 2013, the Executive Office of the United States Attorneys ("EOUSA"), in a two-part referral, referred a total of 535 pages of records to the Criminal Division as it determined the records in question were authored by and maintained by the Criminal Division. Part one of EOUSA's referral to the Criminal Division consisted of three documents, the Memo of February 27, 2012 (See Exhibit 2, "CRM One"), the Memo of July 5, 2012 (See Exhibit 2, "CRM Two"), and an Electronic Communication ("EC"), including the Memo of September 12, 2008, as an attachment thereto (See Exhibit 2, "CRM Three"). Part two of EOUSA's referral to the Criminal Division consisted of records maintained at USABook, a DOJ intranet site (See Exhibit 2, CRM Four and Five). EOUSA requested that the Criminal Division review the documents referred and directly respond to ACLU-NC. EOUSA further advised the Criminal Division that a response to ACLU-NC was required by March 23, 2013.

9. The FOIA/PA Unit received EOUSA's referral and began processing the three memoranda and the sections of USABook that had been referred to it. FOIA/PA Unit personnel conducted a line by line review of the CRM One, CRM Two, CRM Three, and the sections of USABook ("CRM Four and CRM Five"), to determine whether any FOIA exemptions were applicable to the information contained therein and, if so, whether any nonexempt information could be segregated and released to the requester.

Responsive, Non-Exempt Information Disclosed

10. Based on the FOIA/PA Unit's review, it determined that CRM One could be released in part, with two-pages released in full, two-pages released with certain redactions pursuant to FOIA Exemptions 5 and 7(E), and fifty-three pages withheld in full pursuant to FOIA Exemptions 5 and 7(E). Furthermore, the FOIA/PA Unit determined that CRM Two could be released in part, with one-page released with certain redactions pursuant to FOIA Exemptions 5 and 7(E), and fifty-three pages withheld in full pursuant to Exemptions 5 and 7(E). The FOIA/PA Unit concluded that one-hundred and sixteen pages of records comprising CRM Three, CRM Four, and CRM Five needed to be withheld in full pursuant to FOIA Exemptions 5, (b) 6, 7(C) and 7(E). Finally, three-hundred and four pages of records are non-responsive, as they relate to such matters as electronic surveillance, pen register, and trap and trace applications generally.

11. By letter dated March 22, 2013, the Criminal Division notified the plaintiffs of the Criminal Division's disclosure determinations, and provided it with copies of the redacted CRM One and the redacted CRM Two. The Criminal Division further advised the plaintiffs that five-hundred and thirty pages of records were being withheld in full pursuant to FOIA Exemptions 5, 6, 7(C) and 7(E). A true and correct copy of the March 22, 2013 letter to plaintiffs is attached as Exhibit 3.

Exempt Information Withheld

12. The Criminal Division is withholding all other responsive law enforcement records based on FOIA Exemptions 5, 6, 7(C) and 7(E), 5 U.S.C. §§ 552(b)(5), (b)(6), (b)(7)(C)

and (b)(7)(E) (2006 & Supp. 2010). The Criminal Division's Vaughn index describing the information being withheld and the applicable exemptions is attached as Exhibit 2. Our bases for applying particular exemptions to withhold the information described in the Vaughn index are outlined below.

FOIA Exemption 5

Attorney Work Product Doctrine

13. The Criminal Division determined that the records requested by the plaintiffs were exempt under FOIA Exemption 5, which permits agencies to withhold "inter- or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency" (i.e., attorney-client communications, attorney work product, and deliberative process materials). 5 U.S.C. § 552(b)(5). Inasmuch as the records plaintiffs seek were created and exchanged within DOJ, there can be no question that they are "intra-agency," and therefore, fall within the threshold of Exemption 5.

14. The attorney work-product doctrine of FOIA Exemption 5 shields materials prepared by or at the direction of an attorney in reasonable anticipation of litigation. The anticipated litigation can include criminal matters as well as civil and administrative proceedings, and courts have concluded that protection extends to documents prepared in anticipation of both pending litigation and foreseeable litigation even where no specific claim is contemplated. Litigation need not come to fruition in order for the doctrine to attach. The doctrine protects any part of a document prepared in anticipation of litigation, not just the portions concerning opinions and legal theories, and is intended to protect an attorney's opinions, thoughts, impressions, interpretations, and analyses.

15. CRM One, CRM Two and CRM Three were prepared in anticipation of litigation by DOJ officials, and fall squarely within the attorney work product doctrine of Exemption 5. Specifically, CRM One and CRM Two were authored by the Chief of the Criminal Division's Appellate Section, were directed to federal prosecutors, and the purpose of these memoranda was to analyze the possible implications of the Supreme Court decision in

United States v. Jones, 132 S. Ct. 945 (2012) ("*Jones*") on ongoing federal criminal prosecutions and investigations that could result in litigation. The memoranda's author intended for the memoranda to be used as an aid for federal prosecutors in their current and future litigations. To that end, the memoranda identify factual information regarding specific types of techniques employed in current and past criminal investigations. CRM One specifically addresses cases involving GPS tracking devices, and CRM Two addresses cases involving other investigative techniques employed by DOJ. Both memoranda discuss potential legal strategies, defenses, and arguments that might be considered by federal prosecutors in light of *Jones* in each type of case discussed. The memoranda incorporate DOJ attorneys' opinions and impressions of *Jones* and legal analysis of potential claims. Because the memoranda identify specific techniques used in ongoing investigations and legal strategies that might be employed in the cases involving such techniques, the release of these memoranda would fairly be expected to adversely affect DOJ's handling of pending and impending litigation. CRM Three, authored by an associate director of DOJ's Office of Enforcement Operations, provides guidance to federal prosecutors concerning requests for historical cellular telephone location information. The purpose behind CRM 3 was to analyze the implications of an adverse U.S. district court decision cited as *In re Application*, 534 F. Supp. 2d 585 (W.D. Pa. 2008), on ongoing federal criminal prosecutions and investigations that could result in litigation. CRM Three's author intended for the memoranda to be used as an aid for federal prosecutors in their current and future litigations. CRM Three also identifies factual information regarding specific types of techniques employed in current and past criminal investigations. CRM Three discusses potential legal strategies, defenses, and arguments that might be considered by federal prosecutors in light of *In re Application*, *supra*. Because CRM Three identifies specific techniques used in ongoing investigations and legal strategies that might be employed in the cases involving such techniques, the release of this memorandum would fairly be expected to adversely affect DOJ's handling of pending and impending litigation.

16. CRM Four and CRM Five are relevant sections of "USABook," found on a DOJ intranet site. USABook functions as a legal resource book or reference guide for federal

prosecutors. USABook contains up-to-date legal analysis and guidance of specific legal topics germane to federal prosecutors. USABook also contains an appendix with forms or go-bys useful to federal prosecutors, designed to aid them in their current and future litigation. USABook also identifies factual information regarding specific types of investigative techniques employed in current and past criminal investigations. USABook further discusses potential legal strategies, defenses, and arguments that might be considered by federal prosecutors with respect to electronic surveillance, tracking devices and non-wiretap electronic surveillance. Because the USABook identifies specific techniques used in ongoing investigations and legal strategies that might be employed in the cases involving such techniques, the release of this information would fairly be expected to adversely affect DOJ's handling of pending and impending litigation.

Application of FOIA Exemption 7(E)

17. FOIA Exemption 7 exempts from mandatory disclosure "records or information compiled for law enforcement purposes" when disclosure could reasonably be expected to cause one of the harms enumerated in the subparts of the exemption. *See* 5 U.S.C. § 552(b)(7). In order to assert FOIA Exemption 7, an agency must first demonstrate that the records or information that it seeks to withhold were compiled for law enforcement purposes. Law enforcement agencies such as DOJ must demonstrate that the records at issue are related to the enforcement of federal laws and that the enforcement activity is within the law enforcement duty of that agency.

18. CRM One through CRM Five were compiled to address specific issues involving electronic surveillance, tracking devices and non-wiretap electronic surveillance as these issues relate to prospective federal criminal prosecutions and investigations that are within the authority of DOJ to conduct and to aid federal law enforcement personnel in conducting such prosecutions and investigations. Thus, CRM One through CRM Five were compiled for law enforcement purposes and readily meet the threshold requirement of FOIA Exemption 7.

19. Among the subparts of FOIA Exemption 7 is 5 U.S.C. § 552(b)(7)(E), which exempts from disclosure:

> records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

20. In addition to Exemption 5, the FOIA/PA Unit's review of CRM One through CRM Five determined that portions of these documents contain information exempt from disclosure under FOIA Exemption 7(E).

21. CRM One discusses the ways in which GPS tracking devices are employed in federal criminal investigations. The specific techniques available to prosecutors, the circumstances in which such techniques might be employed, and the legal considerations related to such techniques are reflected throughout the document. CRM One thus describes law enforcement techniques and procedures, as well as guidelines for law enforcement investigations and prosecutions that are not publicly known. The disclosure of this information could provide individuals with information that would allow them to violate the law while evading detection by federal law enforcement.

22. CRM Two discusses the ways in which investigative techniques apart from GPS tracking devices are employed in federal criminal investigations. The specific techniques available to prosecutors, the circumstances in which such techniques might be employed, and the legal considerations related to such techniques are reflected throughout the document. CRM Two thus describes law enforcement techniques and procedures, as well as guidelines for law enforcement investigations and prosecutions that are not publicly known. The disclosure of this information could provide individuals with information that would allow them to violate the law while evading detection by federal law enforcement.

23. CRM Three discusses the ways in which investigative techniques involving requests for historical cellular telephone location information are employed in federal criminal investigations. The specific techniques available to prosecutors, the circumstances in which such

techniques might be employed, and the legal considerations related to such techniques are reflected throughout the document. CRM Three thus describes law enforcement techniques and procedures, as well as guidelines for law enforcement investigations and prosecutions that are not publicly known. The disclosure of this information could provide individuals with information that would allow them to violate the law while evading detection by federal law enforcement.

24. CRM Four and CRM Five address specific issues involving electronic surveillance, tracking devices and non-wiretap electronic surveillance as these issues relate to prospective federal criminal prosecutions and investigations that are within the authority of DOJ to conduct and to aid federal law enforcement personnel in conducting such prosecutions and investigations. The specific techniques available to prosecutors, the circumstances in which such techniques might be employed, and the legal considerations related to such techniques are reflected throughout the document. CRM Four and CRM Five thus describe law enforcement techniques and procedures, as well as guidelines for law enforcement investigations and prosecutions that are not publicly known. The disclosure of this information could provide individuals with information that would allow them to violate the law while evading detection by federal law enforcement.

FOIA Exemptions 6 and 7(C) Privacy Interests

25. Information protected from disclosure pursuant to the FOIA's personal privacy exemptions were withheld in CRM Three through CRM Five. Exemption 6 exempts from disclosure "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personnel privacy." 5 U.S.C. § 552(b)(6). Exemption 7(C) safeguards from disclosure "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C).

Balancing Test: Privacy Interests of Individuals versus Public Interest in Disclosure

26. In order to withhold information pursuant to these two exemptions, the Criminal Division must balance the privacy interests of the individuals mentioned in these records against any public interest in disclosure, and find that the balance weighs in favor of non-disclosure. For purposes of this analysis, a public interest exists when information would shed light on the Criminal Division's performance of its statutory duties. In each instance where information was withheld pursuant to Exemptions 6 and 7(C), the Criminal Division determined that the individuals' privacy interests outweighed the dearth of public interest in the information.

27. The Criminal Division examined CRM Three through CRM Five, which contain the names and identifying information of DOJ attorneys involved in the creation of the documents. The Criminal Division could not identify any discernible public interest. In particular, the Criminal Division could not determine how the disclosure of the names and identifying information of these individuals would shed any light on how the Criminal Division executes its statutory duties. Thus, the Criminal Division determined that the privacy interests of these individuals in protecting their names and identifying information from disclosure outweighed any public interest in disclosure, and that disclosure of the names and identifying information would constitute a clearly unwarranted and unwarranted invasion of personal privacy. As such, the Criminal Division properly withheld this information pursuant to Exemptions 6 and 7(C).

Segregability

28. Following a line-by-line review, all reasonably segregable, non-exempt information has been released in full or in part to the plaintiff. The documents withheld in their entirety contain no meaningful portion that could be released without destroying the integrity of the document or without disclosing third-party interests.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this 6th day of June, 2013.

John E. Cunningham III

EXHIBIT 2

NOS. 13-50572, 13-50578, 13-50580, 14-50051

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

BASAALY SAEED MOALIN,
MOHAMED MOHAMED MOHAMUD,
ISSA DOREH,
AHMED NASIR TAALIL MOHAMUD,

DEFENDANTS-APPELLANTS.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA
THE HONORABLE JEFFREY T. MILLER, SENIOR U.S. DISTRICT JUDGE

ANSWERING BRIEF OF PLAINTIFF-APPELLEE

LAURA E. DUFFY
UNITED STATES ATTORNEY
SOUTHERN DISTRICT OF CALIFORNIA
CAROLINE P. HAN
ASSISTANT UNITED STATES ATTORNEY
FEDERAL OFFICE BUILDING
880 FRONT STREET
ROOM 6293
SAN DIEGO, CA 92101-8893
TELEPHONE: (619) 546-6968

JOHN P. CARLIN
ASSISTANT ATTORNEY GENERAL
FOR NATIONAL SECURITY
JEFFREY M. SMITH
APPELLATE COUNSEL
NATIONAL SECURITY DIVISION
U.S. DEPARTMENT OF JUSTICE
950 PENNSYLVANIA AVE, NW
ROOM 6500
WASHINGTON, DC 20530
TELEPHONE: (202) 532-0220

TABLE OF CONTENTS

program without losing important counterterrorism capabilities, the FREEDOM Act delayed the effective date of both of these changes until 180 days after enactment. *See id.* § 109. The former program thus continued with FISC approval, *see In re Application V*, 2015 WL 5637562, until November 29, 2015. As of that time,[9] the NSA was required to proceed under the new statutory framework established by the FREEDOM Act. Under the new framework, the government does not collect telephony metadata in bulk, but instead may apply to the FISC for "production on an ongoing basis of call detail records created before, on, or after the date of the application" for a "specific selection term" (such as a telephone number) where there is "a reasonable, articulable suspicion" that the specific selection term is associated with a foreign power, or an agent of a foreign power, engaged in international terrorism." 50 U.S.C. § 1861(b)(2)(C); *see also id.* § 1861(c)(2)(F).

SUMMARY OF ARGUMENT

The defendants' attack on the NSA's discontinued telephony metadata collection program, through their challenge to the district court's denial of their motion for a new trial, misses the mark. Not only are their arguments challenging the legality of that program meritless, as the district court correctly found, but the

[9] With FISC approval, the NSA continued to maintain access to the bulk call detail records for certain limited, non-analytic, technical purposes for only three additional months, until February 29, 2016. *See Smith v. Obama*, __ F.3d __, 2016 WL 1127087, at *1 (9th Cir. Mar. 22, 2016) (holding that civil claim for injunctive relief against the program was moot).

evidence of the defendants' guilt was neither obtained from the program nor was it the "fruit" of that program. Moreover, the high societal costs of suppression could not be justified in a case where the government acted in good faith in reliance on orders repeatedly issued by Article III courts and where the challenged program has ceased. Denial of the new trial motion was not an abuse of discretion.

The defendants' other arguments fare no better. The district court correctly found that the government had met its *Brady* and other discovery obligations. The district court's evidentiary decisions were well within that court's discretion, and they afforded the defendants a full and fair opportunity to place their defense before the jury. Finally, the evidence was sufficient to support the convictions of all of the defendants, including Issa Doreh, the only defendant who raises this challenge on appeal.

ARGUMENT

I. The District Court's Denial of the Defendants' Motion for a New Trial Was Correct and Not an Abuse of Discretion

The defendants first raised a challenge to the NSA telephony collection program in their September 2013 motion for a new trial. CR345. Their argument for a new trial was complex. They claimed that (1) information about a San Diego-based telephone number was obtained from the allegedly unlawful NSA program; (2) this information prompted a "tip" to the FBI; (3) the FBI then opened an investigation; (4) the FBI's investigation determined that the San Diego-based telephone number

was used by Moalin; (5) the FBI then obtained authorization from the FISC, pursuant to Title I of FISA, to engage in electronic surveillance of Moalin; (6) this FISC-authorized electronic surveillance resulted in the interception of telephone conversations that inculpated the defendants in the conspiracy to support al-Shabaab; and (7) those conversations formed key evidence of the defendants' guilt at trial.[10] The defendants' legal argument was essentially that the NSA program was what is known in Fourth Amendment law as a "poisonous tree," and that the evidence of guilt introduced at trial was its "fruit," and therefore was subject to suppression. Because the trial involved the use of what the defendants argued was "fruit" of a "poisonous tree," they claimed that they were entitled to a new trial. The district court rejected this argument, and this Court should as well.

Moalin's[11] argument contains numerous flaws. For one thing, there is no "poisonous tree." The NSA program was legal. As the district court correctly held,

---

[10] Steps 5, 6, and 7 accurately summarize what occurred. Relevant foreign intelligence investigatory activity that preceded the FISC Title I authorization for electronic surveillance is summarized in the government's classified supplemental brief.

[11] The defendants' brief purports to bring this challenge on behalf of all four defendants. However, defendants Mohamud, Doreh, and Ahmed Nasir lack even a colorable basis to join this challenge as there is no evidence in the record indicating any collection of metadata concerning their calls or, more importantly, that any such collection had any connection whatsoever to the prosecution of the defendants. *See Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (only a person whose rights were violated can pursue remedy); *Alderman v. United States,* 394 U.S. 165, 171-75 (1969) (same); *see also Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015) (holding that plaintiffs who

(continued . . .)

Moalin's Fourth Amendment challenge runs squarely against clear, binding precedent from both the Supreme Court and this Court holding that there is no reasonable expectation of privacy in telephony metadata records held by the phone company. Moalin's statutory suppression argument is also without merit, and, in any event, there is no suppression remedy for the statutory violation that Moalin alleges.

But this Court need not even reach these questions because, for at least three separate reasons, the evidence introduced at trial in this case was not "fruit" of the challenged NSA program. *See United States v. Crawford*, 372 F.3d 1048, 1053-59 (9th Cir. 2004) (en banc) (finding that attenuation doctrine precluded suppression without deciding whether there was an underlying constitutional violation); *see also Lyng v. Nw. Indian Cemetery Protective Ass'n*, 485 U.S. 439, 445 (1988) ("A fundamental and longstanding principle of judicial restraint requires that courts avoid reaching constitutional questions in advance of the necessity of deciding them."). First, an investigative lead or tip does not taint the entire subsequent investigation, as the intervening investigative steps serve to attenuate the evidence. *United States v. Smith*, 155 F.3d 1051, 1063 (9th Cir. 1998). Second, by themselves, the FISC orders authorizing the Title I surveillance attenuate the evidence from the initial "tip." *Segura v. United States*, 468 U.S. 796, 813-16 (1984). And, third, the classified record

(. . . continued)
merely speculated that metadata relating to their calls had been collected by NSA lacked standing to maintain civil challenge to collection).

provides an additional reason why the trial evidence was not "fruit" of the NSA program.

Moreover, there are two additional reasons why suppression was unavailable in this case. First, suppression is precluded where government agents were acting based on facially valid court orders such as those that authorized the NSA program. *See United States v. Leon*, 468 U.S. 897, 925 (1984); *cf. United States v. Craig*, 861 F.2d 818, 820 (5th Cir. 1988) ("Principles of judicial restraint and precedent dictate that, in most cases, we should not reach the probable cause issue if a decision on the admissibility of the evidence under the good-faith exception of *Leon* will resolve the matter."). And, second, suppression is not appropriate where, as here, it could serve no deterrence function because the challenged program has ended and there is no prospect of it restarting. *United States v. Dreyer*, 804 F.3d 1266, 1280 (9th Cir. 2015) (en banc).

A. Standard of Review

A district court's decision not to grant a new trial is reviewed for abuse of discretion. *United States v. Young*, 17 F.3d 1201, 1203 (9th Cir. 1994). The district court's factual findings are reviewed for clear error. *United States v. Orman*, 486 F.3d 1170, 1173 (9th Cir. 2007). Questions of law relating to suppression are reviewed *de novo*. *Id.*

B. The Evidence Presented at Trial Was Not "Fruit" of the Challenged NSA Program Because an Investigatory Lead Cannot Taint an Entire Investigation

Even assuming that there was a causal chain linking the NSA program and the evidence introduced at trial, there is no doubt that the trial evidence was attenuated from the tip generated by the telephony metadata program. But-for causation is a "necessary, [but] not a sufficient, condition for suppression." *Hudson v. Michigan*, 547 U.S. 586, 592 (2006); *see also United States v. Ankeny*, 502 F.3d 829, 837 (9th Cir. 2007). Indeed, the Supreme Court has repeatedly held that "but-for cause, or 'causation in the logical sense alone,' . . . can be too attenuated to justify exclusion." *Hudson v. Michigan*, 547 U.S. at 592 (quoting *United States v. Ceccolini*, 435 U.S. 268, 274 (1978)); *accord United States v. Smith*, 155 F.3d 1051, 1060 (9th Cir. 1998) (reaffirming "the courts' consistent rejection of a 'but for' causation standard in 'fruit of the poisonous tree' doctrine"). Thus, even where but-for causation has been established, a court must further determine "whether, granting establishment of the primary illegality, the evidence . . . has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." *Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *see also Brown v. Illinois*, 422 U.S. 590, 603-04 (1975).

As the defendants concede, the relevant product of the NSA program was merely a "tip," D.Br. 115, that provided law enforcement with the impetus to look into a phone number that turned out to have been used by Moalin. As a matter of

law, such a tip or lead, even where (unlike here) it is unlawfully obtained, cannot taint an entire criminal investigation or the resulting criminal conviction. *United States v. Smith*, 155 F.3d 1051, 1063 (9th Cir. 1998). A holding to the contrary would "grant life-long immunity from investigation and prosecution simply because a violation of the Fourth Amendment first indicated to the police that a man was not the law-abiding citizen he purported to be." *United States v. Cella*, 568 F.2d 1266, 1285-86 (9th Cir. 1977) (quoting *United States v. Friedland*, 441 F.2d 855, 861 (2d Cir. 1971) (Friendly, J.)); *accord United States v. Ortiz–Hernandez*, 427 F.3d 567, 577 (9th Cir. 2005) ("[A] criminal defendant cannot suppress his identity, even when there has been some prior illegality on the part of the government.").

In *United States v. Smith*, this Court found that the government had illegally accessed a voicemail message from the defendant that suggested that he was involved in insider trading. 155 F.3d at 1053-54. This voicemail led the Securities and Exchange Commission to investigate the defendant, and he was eventually convicted of securities laws violations. *Id.* at 1054. The defendant argued that because the unlawfully obtained voicemail "was the impetus for starting the investigation," therefore "the evidence obtained in the subsequent investigation of [defendant] should have been suppressed." *Id.* at 1060-61 (quoting defendant's brief).

This argument, which is similar to the argument advanced by Moalin in this case, was squarely rejected by this Court: "Contrary to Smith's suggestions, under

Ninth Circuit precedent, the baseline inquiry in evaluating taint is not whether an unlawful search was the 'impetus' for the investigation or whether there exists an unbroken 'causal chain' between the search and the incriminating evidence." *Id.* at 1061. Quite the opposite, "it is *not* sufficient in demonstrating taint . . . that an illegal search uncovers the alleged perpetrator's identity, and therefore directs attention to a particular subject." *Id.* (emphasis in original) (quotation marks omitted). Thus, while the unlawfully acquired voicemail message may have "tipped off the government to the fact that a crime had been committed and to the probable identity of the perpetrator," that was not enough to establish taint through the fruit-of-the-poisonous-tree doctrine. *Id.* at 1063. Rather, the voicemail was "a 'lead'," and a lead "is simply not enough to taint an entire investigation." *Id.*; *accord Hoonsilapa v. INS*, 575 F.2d 735, 738 (9th Cir. 1978) ("[T]he mere fact that [a] Fourth Amendment illegality directs attention to a particular suspect does not require exclusion of evidence subsequently unearthed from independent sources."). The lead in this case was even more limited than the voicemail in *Smith*, as it did not even include Moalin's first or last name, but rather "revealed only the slimmest of leads: [a telephone] number." *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 113 (D.D.C. 2014). Thus, the government "was required to take an additional investigative step just to find a name associated with the [telephone] number, as compared to the typical 'unlawful

lead' case in which the defendant's full identity is discovered through the illegal search or seizure." *Id.*

The law in other circuits is the same. *E.g.*, *United States v. Carter*, 573 F.3d 418, 423 (7th Cir. 2009) ("Few cases, if any, applying the attenuation exception hold that evidence . . . is inadmissible because an illegal search first made a particular person a suspect in a criminal investigation."); *United States v. Najjar*, 300 F.3d 466, 478-79 (4th Cir. 2002) (documents from illegal search led to a subsequent investigation, but additional and independent investigatory steps sufficiently attenuated evidence from initial search); *United States v. Watson*, 950 F.2d 505, 508 (8th Cir. 1991) ("[W]here a law enforcement officer merely recommends investigation of a particular individual based on suspicions arising serendipitously from an illegal search, the causal connection is sufficiently attenuated so as to purge the later investigation of any taint from the original illegality."); *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 112 (D.D.C. 2014) ("Federal courts consistently have held that the exclusionary rule does not apply to subsequently discovered evidence when an initial limited piece of information—typically the name of a potential target for investigation—is obtained through an illegal search or seizure because substantial intervening investigative steps still are required to uncover the necessary incriminating evidence.").

For example, in *United States v. Friedland*, agents illegally bugged the offices of an acquaintance of the defendant. 441 F.2d at 856-57. The agents who conducted the

bugging informed other agents that the defendant was worth investigating, and this triggered further investigation, which uncovered the defendant's involvement in bond forgery. *Id.* at 857. In refusing to suppress the evidence, Judge Friendly held that it "would stretch the exclusionary rule beyond tolerable bounds" to suppress the results of an investigation because an illegal search had led police to focus on the defendant. *Id.* at 861.[12]

Because the NSA program provided a mere tip or lead, it did not taint the evidence that was subsequently uncovered using independent investigatory techniques.

C. The Valid FISC Orders Issued under FISA Title I Attenuated the Trial Evidence from the NSA Program

Evidence seized pursuant to valid judicially-issued process that was based upon information obtained independently from the alleged illegality is not subject to suppression. *See Segura v. United States*, 468 U.S. 796, 813-16 (1984); *United States v. Bosse*, 898 F.2d 113, 116 (9th Cir. 1990); *see also Johnson v. Louisiana*, 406 U.S. 356, 365

[12] The cases relied on by Moalin do not involve tips that provided the impetus for further investigation; they involve the use of illegally obtained substantive evidence to further investigations. *United States v. Perez*, 506 F. App'x 672 (9th Cir. 2013), involved the illegal seizure of a telephone containing "incriminating photographs and text messages." *Id.* at 674. *United States v. Thomas*, 211 F.3d 1186 (9th Cir. 2000), involved an illegal automobile search that uncovered approximately 60 pounds of marijuana and a shotgun. *Id.* at 1188-89. *Commonwealth v. Keefner*, 961 N.E.2d 1083 (Mass. 2012), like *Perez*, involved an unlawful seizure of a telephone. *Id.* at 1092. And *Staples v. United States*, 320 F.2d 817 (5th Cir. 1963), concerned an unlawful automobile search that uncovered a hotel room key. *Id.* at 820.

(1972) (bail hearing before magistrate purged the taint of unlawful arrest such that subsequent lineup was not fruit of poisonous tree).

The trial evidence that Moalin sought to suppress by way of his new trial motion (*i.e.*, the intercepted phone calls) was obtained pursuant to FISC orders issued under Title I of FISA. This intervening judicial authority fully attenuates the trial evidence from the NSA "tip." *See Segura*, 468 U.S. at 814, 816 (even if alleged illegality "could be considered the 'but for' cause for discovery of the evidence," valid intervening search warrant "purge[d] the evidence of any 'taint' arising from the entry").

A different conclusion regarding attenuation might be warranted if information from the telephony metadata program had been necessary for the FISC's probable cause finding. *See Franks v. Delaware*, 438 U.S. 154 (1978). But that is not the case here. The telephony metadata program allowed the government to learn that a telephone number that turned out to be Moalin's had "had indirect contacts with a known terrorist overseas." ER74 (quoting FBI Deputy Director). The program collected no communications content, and the mere fact that Moalin had talked to one or more people who had in turn talked to a known terrorist could not, by itself, support a probable cause finding that Moalin was "a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2)(A). More importantly, in this case, it did not and was not necessary to support the requisite probable cause showing for the FISA

Title I application. This is demonstrated by the classified record available to this Court, which contains the relevant FISC applications. *See also* Gov't Classified Supp. Br. Thus, trial evidence obtained through use of FISA Title I authority in this case was not the "fruit" of the challenged NSA program. *United States v. Karo*, 468 U.S. 705, 719 (1984); *see also United States v. Forrester*, 512 F.3d 500, 513 (9th Cir. 2008); *United States v. Salas*, 879 F.2d 530, 537-38 (9th Cir. 1989).

D. There Is an Additional Reason Why the Evidence Was Not the "Fruit" of the NSA Program

The government's classified supplemental brief provides an additional basis for finding that the evidence admitted at trial was not the "fruit" of the telephony metadata program.

E. There Is No Suppression Remedy for the Statutory Violation that Moalin Posits

Statutory violations do not lead to suppression of evidence unless (1) suppression "is clearly contemplated by the relevant statute," *United States v. Forrester*, 512 F.3d 500, 512 (9th Cir. 2007); *accord United States v. Donovan*, 429 U.S. 413, 432 n.22 (1977) (holding that the availability of a suppression remedy for "statutory, as opposed to constitutional, violations . . . turns on the provisions of [the statute] rather than the judicially fashioned exclusionary rule"), or (2) "the excluded evidence arose directly out of statutory violations that implicated important Fourth and Fifth