No.

In the Supreme Court of the United States

FEDERAL BUREAU OF INVESTIGATION ET AL.,
PETITIONERS

v.

YASSIR FAZAGA, ET AL.

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

APPENDIX TO THE PETITION FOR A WRIT OF CERTIORARI

D. JOHN SAUER
Solicitor General
Counsel of Record
BRETT A. SHUMATE
Assistant Attorney General
SARAH M. HARRIS
Deputy Solicitor General
ANTHONY A. YANG
Assistant to the Solicitor General
SHARON SWINGLE
BRAD HINSHELWOOD
Attorneys
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

TABLE OF CONTENTS

Table of Contents—Continued: Page

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 12-56867
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLEES

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; PAT ROSE;
KEVIN ARMSTRONG; PAUL ALLEN, DEFENDANTS

AND

BARBARA WALLS; J. STEPHEN TIDWELL,
DEFENDANTS-APPELLANTS

No. 12-56874
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLEES

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN

TIDWELL; BARBARA WALLS, DEFENDANTS

AND

PAT ROSE; KEVIN ARMSTRONG; PAUL ALLEN,
DEFENDANTS-APPELLANTS

No. 13-55017

D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLANTS

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN
TIDWELL; BARBARA WALLS; PAT ROSE; KEVIN
ARMSTRONG; PAUL ALLEN; UNITED STATES OF
AMERICA, DEFENDANTS-APPELLEES

Argued and Submitted: June 8, 2023
Seattle, Washington
Filed: Dec. 20, 2024

On Remand from the United States Supreme Court

OPINION

BEFORE: RONALD M. GOULD AND MARSHA S. BERZON, CIRCUIT JUDGES, AND GEORGE CARAM STEEH III,* DISTRICT JUDGE.

BERZON, Circuit Judge:

This case involves constitutional and statutory claims arising out of the FBI's alleged improper surveillance of Muslims in Southern California. We revisit it after a remand from the Supreme Court. The Court reversed our prior conclusion that the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1806(f), displaced the state secrets privilege and its dismissal remedy with respect to electronic surveillance. *See Fazaga v. FBI*, 965 F.3d 1015 (9th Cir. 2020), *rev'd*, 595 U.S. 344, 355, 359 (2022). The issues before us now are (i) whether to address the *Bivens* claims asserted against the individual defendants, which we declined to do in our earlier opinion, and if we do so, how to resolve them, and (ii) whether the state secrets privilege requires dismissal of Fazaga's religion claims at the motion to dismiss stage.

We hold this time around that the *Bivens* claims should be dismissed. The Supreme Court's jurisprudence since our earlier consideration of this case establishes that no *Bivens* cause of action is cognizable on the facts alleged.

As to the religion claims, we affirm the district court's determination that the government properly invoked the state secrets evidentiary privilege under *United States v. Reynolds*, 345 U.S. 1 (1953), and that at least some of the information the government describes

---

* The Honorable George Caram Steeh III, United States District Judge for the Eastern District of Michigan, sitting by designation.

is privileged. But we conclude that the application of that privilege does not warrant dismissal of the claims at this juncture. The government has not demonstrated that excluding the privileged information would deprive it of a valid defense or that the privileged information is so intertwined with the relevant nonprivileged information that further litigation unacceptably risks disclosing state secrets. We therefore reverse the dismissal of the religion claims and remand those claims to the district court to consider how the case should proceed.

I.

Here is a brief summary of the factual background of this case:

The plaintiffs—Yassir Fazaga, Ali Malik, and Yasser AbdelRahim (collectively, "Fazaga")—are three Muslim residents of Southern California. They allege that, as part of a counterterrorism investigation known as "Operation Flex," the FBI paid a confidential informant, Craig Monteilh, to gather information about Muslims. The operative complaint states that Operation Flex was a "dragnet surveillance" program that targeted them and other Muslims "solely due to their religion." In accordance with an expansive directive to gather information on Muslims generally, Monteilh engaged with a broad range of Muslim people at mosques, community events, gyms, and other settings, and recorded virtually all of his interactions.

Fazaga filed a putative class action against the United States, the FBI, and two FBI leaders in their official capacities (collectively, "the government"), and against five FBI agents in their individual capacities

("the agent defendants").[1] The operative complaint asserts eleven causes of action of two types: (i) claims alleging unconstitutional searches in violation of the Fourth Amendment and the Foreign Intelligence Surveillance Act (FISA), and (ii) claims alleging religious discrimination, burdens on religion, and other violations of Fazaga's religious freedom rights under the First and Fifth Amendments, the Privacy Act, the Religious Freedom Restoration Act (RFRA), and the Federal Tort Claims Act (FTCA). Fazaga seeks an injunction "ordering Defendants to destroy or return any information gathered through the unlawful surveillance program," as well as compensatory and punitive damages against the agent defendants.

Central to Fazaga's case is Monteilh, whom the government acknowledges was a confidential informant. The record contains extensive public declarations by Monteilh detailing his interactions with Fazaga and others. Fazaga's complaint also references news reporting on Monteilh's activities. The government does not maintain that the information in Fazaga's complaint or Monteilh's declarations is privileged or classified. This case thus arises with a considerable amount of information related to Fazaga's religious discrimination claims already public and unprivileged.

The Attorney General of the United States invoked the state secrets privilege with respect to three categories of potential evidence. In support of its privilege assertion, the government filed public declarations from

---

[1] The putative class includes "[a]ll individuals targeted by Defendants for surveillance or information-gathering through Monteilh and Operation Flex, on account of their religion, about whom the FBI thereby gathered personally identifiable information."

the Attorney General and from the Assistant Director of the FBI's Counterterrorism Division. It also provided two classified declarations from the Assistant Director and a classified supplemental memorandum, which the district court, and we, reviewed *ex parte* and *in camera*.

The government moved to dismiss Fazaga's religion claims pursuant to the state secrets privilege, as well as on other grounds. The agent defendants moved to dismiss all the claims against them on various grounds. The district court dismissed all of Fazaga's non-FISA claims on the basis of the state secrets privilege—including the Fourth Amendment claim, although the government had not sought its dismissal on privilege grounds.

On appeal, we reversed the district court's dismissal of certain claims and affirmed the dismissal of others. Relevant here, we held that FISA's procedures for challenging electronic surveillance, 50 U.S.C. § 1806(f), applied in lieu of the state secrets privilege and its dismissal remedy with respect to such surveillance. *Fazaga*, 965 F.3d at 1052. Having done so, we concluded that certain of the religion claims against the government defendants could go forward.[2] *Id.* at 1064-65. We declined to address whether the *Bivens* claims against the agent defendants survived. *Id.* at 1055-59.

The Supreme Court reversed the case on the "narrow" ground that FISA "does not displace the state secrets

---

[2] Specifically, we reversed the dismissal of the First and Fifth Amendment and RFRA claims. 965 F.3d at 1056-64. We did not address on the merits Fazaga's FTCA claims because the "applicability of the discretionary function exception [to the FTCA] will largely turn on the district court's ultimate resolution of the merits of Plaintiffs' various federal constitutional and statutory claims." *Id.* at 1065.

privilege" and remanded. *Fazaga*, 595 U.S. at 355, 359. The Court expressly did not "decide whether the Government's evidence is privileged or whether the District Court was correct to dismiss respondents' claims on the pleadings." *Id.* And the Court did not address any aspect of our opinion not involving the state secrets doctrine.

We ordered, and the parties filed, supplemental briefing addressing, among other things, which issues should be considered by this panel on remand. The remaining issues have narrowed considerably, to (i) whether the *Bivens* claims against the agent defendants may go forward in light of the Supreme Court's recent *Bivens* jurisprudence, and (ii) whether the remaining religion claims should be dismissed on the basis of the state secrets privilege. We address each issue in turn.

II.

In our earlier opinion we declined to reach the *Bivens* claims. We now revisit that decision in light of later case law.

Relying on *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971), Fazaga seeks monetary damages against the agent defendants for the alleged Fourth Amendment search violation and for his First and Fifth Amendment religious discrimination claims. In our previous opinion, we held with respect to the search issues that, "[i]n light of the overlap between the [Fourth Amendment] *Bivens* claim and the narrow range of the remaining FISA claim against the Agent Defendants that can proceed, it is far from clear that Plaintiffs will continue to press this claim." *Fazaga*, 965 F.3d at 1056. And as to the First and Fifth Amendment *Bivens* claims, we held that only those claims premised on alleged "conduct motivated by intentional discrimination against

Plaintiffs because of their Muslim faith" could proceed.[3] *Id.* at 1058-59. We remanded the issue to the district court to determine whether a *Bivens* remedy is available for any of the surviving claims. *Id.* at 1056, 1059.

The Supreme Court has, since our earlier opinion, clarified the limited availability of *Bivens* remedies, obviating the need to remand to the district court. *See Egbert v. Boule*, 596 U.S. 482 (2022). *Egbert* forecloses a *Bivens* remedy for any of the remaining *Bivens* claims against the agent defendants. "[U]nder *Egbert* in all but the most unusual circumstances, prescribing a cause of action is a job for Congress, not the courts. This case is not the rare exception." *Mejia v. Miller*, 61 F.4th 663, 669 (9th Cir. 2023) (internal quotation marks and citation omitted).

Before *Egbert*, the Supreme Court had set out a two-step inquiry for evaluating a *Bivens* claim. "First, we ask whether the case presents a new *Bivens* context—i.e., is it meaningfully different from the three cases in which the Court has implied a damages action."[4] *Egbert*, 596 U.S. at 492 (quoting *Ziglar v. Abbasi*, 582 U.S. 120, 139 (2017)) (internal quotation marks and alterations

---

[3] We held earlier that no *Bivens* remedy was available for Plaintiffs' religion claims to the extent they were premised on the agent defendants' alleged improper collection and retention of information about the Plaintiffs, or on the burden of that surveillance on Plaintiffs' exercise of religion. *Fazaga*, 965 F.3d at 1057-58. The Privacy Act and RFRA, "taken together, function as an alternative remedial scheme" for those claims, we held, *id.* at 1059, so a *Bivens* remedy is unavailable, *id.* at 1057; *Ziglar v. Abbasi*, 582 U.S. 120, 137 (2017).

[4] Namely, *Bivens*, 403 U.S. 388; *Davis v. Passman*, 442 U.S. 228 (1979); and *Carlson v. Green*, 446 U.S. 14 (1980). *See Ziglar*, 582 U.S. at 131.

omitted). Second, if the context is new, we consider whether "there are 'special factors' indicating that the Judiciary is at least arguably less equipped than Congress to 'weigh the costs and benefits of allowing a damages action to proceed.'" *Id.* (quoting *Ziglar*, 582 U.S. at 136). If so, no *Bivens* remedy is available.

Egbert explained that these two steps "often resolve to a single question: whether there is any reason to think that Congress might be better equipped to create a damages remedy." 596 U.S. at 492. Since *Bivens* was decided, "expanding the *Bivens* remedy" to other contexts has become "a disfavored judicial activity." *Ziglar*, 582 U.S. at 135 (quotation marks omitted). Under *Egbert*, "*any* rational reason (even one) to think that *Congress* is better suited to weigh the costs and benefits of allowing a damages action" precludes a *Bivens* claim. 596 U.S. at 496 (internal quotation marks omitted).

A.

Applying *Egbert*, we are constrained to conclude that no *Bivens* remedy is available for Fazaga's First and Fifth Amendment religion claims.

First, these claims arise in an entirely new context. The Supreme Court has "never held that *Bivens* extends to First Amendment claims." *Egbert*, 596 U.S. at 498 (internal quotation marks omitted). And, although the Supreme Court recognized a *Bivens* remedy for violations of the Fifth Amendment's Equal Protection Clause in *Davis v. Passman*, 442 U.S. 228 (1979), that case involved a "meaningfully different" context. *Egbert*, 596 U.S. at 492 (internal quotation marks and alterations omitted). In *Davis*, the Supreme Court inferred a damages claim against a member of Congress who allegedly terminated the plaintiff because of her gender. 442 U.S.

at 248-49. In contrast, this case involves FBI agents who conducted a counterterrorism investigation that allegedly discriminated on the basis of religion.

A case presents a new *Bivens* context when it "is different in a meaningful way from previous *Bivens* cases decided by this Court"—for example, if it involves a "new category of defendants" or if "the statutory or other legal mandate under which the officer was operating" differs. *Ziglar*, 582 U.S. at 135, 139-40 (internal quotation marks omitted). Applying a case about an employment decision made by a Congressman to investigative decisions made by law enforcement agents carrying out a national security program in the executive branch would undoubtedly extend *Bivens* to a new context. *Harper v. Nedd*, 71 F.4th 1181, 1187 (9th Cir. 2023), for example, held that a challenge to adverse employment actions by the Bureau of Land Management is a meaningfully different context from *Davis*, although the context, an employment dispute, was considerably closer to *Davis* than here. Not only does this case involve a new category of defendants, but the agent defendants' conduct was carried out under distinct legal mandates to investigate threats to national security, including the Intelligence Reform and Terrorism Prevention Act, 50 U.S.C. § 401 *et seq.*, and Executive Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981). Further, the discrimination alleged was on the basis of religion, rather than on the basis of gender as in *Davis*.

Second, given this new context, several factors weigh against expanding *Bivens* to reach Fazaga's claims—or, put in *Egbert* terms, there is at least one rational reason to believe that Congress is better suited than the judiciary to determine the availability of a damages remedy.

Chiefly, "a *Bivens* cause of action may not lie where, as here, national security is at issue." *Egbert*, 596 U.S. at 494; *see Hernandez v. Mesa*, 589 U.S. 93, 105-09 (2020). Fazaga's claims that he was impermissibly targeted for surveillance on the basis of his religion "challenge more than standard law enforcement operations." *See Ziglar*, 582 U.S. at 142 (internal quotation marks omitted). These claims concern the FBI's counterterrorism operations and so involve "major elements of the Government's whole response to the September 11 attacks, thus of necessity requiring an inquiry into sensitive issues of national security." *See id.* Such "[j]udicial inquiry into the national-security realm raises concerns for the separation of powers in trenching on matters committed to the other branches." *Id.* (internal quotation marks omitted). "[F]ear of personal monetary liability and harassing litigation" may "unduly inhibit officials in the discharge of their duties," *Egbert*, 596 U.S. at 499 (internal quotation marks omitted), presenting a serious concern regarding national security decisionmaking. In that context, FBI agents may need to "tak[e] urgent and lawful action in a time of crisis." *Ziglar*, 582 U.S. at 145.

For these reasons, "the Judiciary is not undoubtedly better positioned than Congress to authorize a damages action in this national-security context." *See Egbert*, 596 U.S. at 495. Under *Egbert*, a *Bivens* remedy for Fazaga's religious discrimination claims is precluded.

B.

For similar reasons, a *Bivens* remedy is not available for Fazaga's Fourth Amendment claim.

This claim too arises in a new context. *Bivens* concerned a Fourth Amendment violation by federal offic-

ers. But "our understanding of a 'new context' is broad." *Hernandez*, 589 U.S. at 102. "A claim may arise in a new context even if it is based on the same constitutional provision as a claim in a case in which a damages remedy was previously recognized." *Id.* at 103. *Bivens* involved an allegedly unconstitutional arrest and physical search of the plaintiff's home. *Bivens*, 403 U.S. at 389. "There is a world of difference" between those claims and Fazaga's Fourth Amendment claim about unlawful surveillance conducted pursuant to the FBI's counterterrorism strategies, "where the risk of disruptive intrusion by the Judiciary into the functioning of other branches is significant." *See Hernandez*, 589 U.S. at 103 (internal quotation marks omitted).

Applying *Hernandez*, we conclude that the national security concerns we've discussed preclude expanding *Bivens* to this new Fourth Amendment context. A *Bivens* remedy against individual FBI agents could have "systemwide consequences" for the FBI's execution of its mandate to protect the United States against terrorist attacks. *See Egbert*, 596 U.S. at 493 (internal quotation marks omitted). The "uncertainty" of the effects of expanding *Bivens* in this manner "alone is a special factor that forecloses relief." *Id.*

Moreover, we previously noted that "the substance of Plaintiffs' Fourth Amendment *Bivens* claim is identical to the allegations raised in their FISA § 1810 claim." *Fazaga*, 965 F.3d at 1055. Thus, an "alternative remedial structure" exists that counsels against fashioning a *Bivens* remedy here. *Egbert*, 596 U.S. at 493 (internal quotation marks omitted).

For these reasons, we affirm the dismissal of the *Bivens* claims.

III.

The remaining issue before us concerns the effect of the government's assertion of the state secrets privilege under *United States v. Reynolds* on Fazaga's religion claims.

The state secrets privilege arises from "the sometimes-compelling necessity of governmental secrecy" to protect national security, which the Supreme Court has recognized "by acknowledging a Government privilege against court-ordered disclosure" of secret "information about . . . military, intelligence, and diplomatic efforts." *Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 484 (2011). The privilege has two distinct applications. The first, set forth in *Totten v. United States*, 92 U.S. 105 (1875), forbids courts to adjudicate claims directly premised on state secrets. This "unique and categorical . . . bar," *Tenet v. Doe*, 544 U.S. 1, 6 n.4 (2005), applies only where "the very subject matter of the action" is itself "a matter of state secret," *Reynolds*, 345 U.S. at 11 n.26. If *Totten* applies, the result is always dismissal. In *Totten*, for example, the Supreme Court affirmed dismissal of a suit against the United States to recover compensation allegedly promised to a Civil War spy, noting that the "existence" of the contract was "itself a fact not to be disclosed" and that litigation would "inevitably lead to the disclosure of matters which the law itself regards as confidential." 92 U.S. at 105-07.

Acknowledging the harshness of categorical dismissal, the Supreme Court recently explained that the *Totten* rule "captures what the *ex ante* expectations of the parties were or reasonably ought to have been. Both parties 'must have understood' . . . that state secrets would prevent courts from resolving many possible dis-

putes under the . . . agreement." *Gen. Dynamics*, 563 U.S. at 490 (quoting *Totten*, 92 U.S. at 106). So the *Totten* bar is rooted in the plaintiff's choice to participate in a matter involving a state secret, the secret nature of which precludes judicial review of ensuing disputes.

The second version of the state secrets privilege, set forth in *Reynolds*, is an evidentiary one. Unlike the *Totten* bar, which always requires dismissal, the *Reynolds* privilege ordinarily requires only that a court "apply[] evidentiary rules: The privileged information is excluded, and the trial goes on without it." *Gen. Dynamics*, 563 U.S. at 485.

Here, the government asserts only the *Reynolds* evidentiary privilege. It seeks to keep secret information that could tend to "confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation"; "reveal the initial reasons . . . for an FBI counterterrorism investigation of a particular person . . . , any information obtained during the course of such an investigation, and the status and results of the investigation"; or "reveal whether particular sources and methods were used in a counterterrorism investigation."

But rather than just seeking exclusion of the assertedly privileged information, the government requested dismissal of the case at the pleading stage, which the district court granted. To review the dismissal, we must decide (a) whether the government has properly invoked *Reynolds* privilege, (b) whether information in the identified categories is in fact privileged, and (c) if it is privileged, whether Fazaga's religion claims must be dismissed as a result, as the government maintains is

necessary to protect the information.[5] *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1080 (9th Cir. 2010) (en banc). We review *de novo* the interpretation and application of the state secrets doctrine and review for clear error the district court's underlying factual findings. *Id.* at 1077.

A.

First, did the government properly invoke the *Reynolds* privilege? Doing so requires a "formal claim . . . by the head of the department which has control over the matter, after actual personal consideration by that officer." *Reynolds*, 345 U.S. at 7-8 (footnote omitted). "To ensure that the privilege is invoked no more often or extensively than necessary," the claim must be a "serious" and "considered" one and "reflect the certifying official's *personal* judgment." *Jeppesen*, 614 F.3d at 1080 (quoting *United States v. W.R. Grace*, 526 F.3d 499, 507-08 (9th Cir. 2008) (en banc)). It must include "sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Id.*

The government has met these requirements. In a public declaration, then-Attorney General Eric Holder asserted the privilege over three categories of information that "could reasonably be expected to cause signifi-

---

[5] The district court dismissed Fazaga's Fourth Amendment claims under the state secrets privilege, although the government expressly did not seek dismissal on that ground. *See Fazaga*, 965 F.3d at 1042-43. We previously held that this dismissal was erroneous because the government had not formally invoked the state secrets privilege as to those claims. *See id.* The Supreme Court did not address this portion of our holding and the parties do not now challenge it, so it remains in effect.

cant harm to the national security" if disclosed, based on his "personal consideration of the matter." We are satisfied that this declaration and the supporting public and classified declarations by an FBI counterterrorism official include sufficient detail for this courts' review.[6]

Fazaga challenges this privilege assertion because the Attorney General declared that he had considered "the matter" but did not say that he had reviewed the underlying source material. This argument fails. The declaration reflects *Reynolds*' instruction that the privilege must be claimed "by the head of the department which has control over *the matter*, after actual personal consideration." 345 U.S. at 8 (emphasis added) (footnote omitted). The official need not have reviewed every piece of information to validly invoke the privilege. "[O]nce [an official] has . . . adequately identified categories of privileged information, [she] cannot reasonably be expected personally to explain why each item . . . responsive to a discovery request affects the national interest." *Kasza v. Browner*, 133 F.3d 1159, 1169 (9th Cir. 1998).

In sum, the Attorney General properly invoked the *Reynolds* privilege.

---

[6] In 2022, after the Justice Department supplemented the internal procedures for invoking the state secrets privilege in effect at the time of the privilege assertion in this case, the government informed us that, based on another round of review, it had again "concluded that invocation of the privilege and dismissal of certain claims remained necessary to protect national security." *See* Memorandum from the Att'y Gen. on Policies & Procedures Governing Invocation of the State Secrets Privilege (Sept. 23, 2009), perma.cc/FRX3-5U5J; Memorandum from Att'y Gen. on Supplement to Policies & Procedures Governing Invocation of the State Secrets Privilege (Sept. 30, 2022), perma.cc/25QX-6PLL.

B.

Next, was the information at issue in fact privileged? The state secrets privilege has been held generally to apply to information that would result in "impairment of the nation's defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign governments, or where disclosure would be inimical to national security." *Fazaga*, 965 F.3d at 1040-41 (quoting *Black v. United States*, 62 F.3d 1115, 1118 (8th Cir. 1995)). We will sustain a privilege claim if we determine "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10. Though "*in camera* review is not always required," *United States v. Zubaydah*, 595 U.S. 195, 205-06 (2022), "[s]ufficient detail must be . . . provided for us to make a meaningful examination," *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007).

Fazaga does not dispute that the identified categories encompass at least some privileged information. But "we must make an independent determination whether the information is privileged" and "assure [ourselves] that an appropriate balance is struck between protecting national security matters and preserving an open court system." *Jeppesen*, 614 F.3d at 1081 (quoting *Al-Haramain*, 507 F.3d at 1202-03).

As we have explained, the government here asserts the state secrets privilege over three categories of information pertaining to FBI counterterrorism investigations: (i) "[i]nformation that could tend to confirm or deny whether a particular individual was or was not

the subject of an FBI counterterrorism investigation"; (ii) "[i]nformation that could tend to reveal the initial reasons (i.e., predicate) for an FBI counterterrorism investigation of a particular person (including in Operation Flex), any information obtained during the course of such an investigation, and the status and results of the investigation"; and (iii) "[i]nformation that could tend to reveal whether particular sources and methods were used in a counterterrorism investigation." These categories of information "indisputably are matters that the state secrets privilege may cover." *See Jeppesen*, 614 F.3d at 1086. We have carefully examined the government's public and classified declarations and classified supplemental briefs in support of its privilege claim, all of which were reviewed by the district court as well.[7] We also held an *ex parte*, *in camera* argument with the government defendants' counsel immediately after the public argument regarding the assertedly privileged information. Having done so, we are convinced that the disclosure of at least some information within the three identified categories would seriously harm legitimate national interests and so is privileged.

C.

Finally, given our conclusion that at least some of the information at issue in this case is privileged, how should this case proceed?

1.

Normally the *Reynolds* privilege operates like any other evidentiary privilege: the privileged information

---

[7] The government's classified disclosures to the court do not include the underlying source material but provide detailed accounts of that material.

does not come in and the case goes on without it. "Ordinarily, simply excluding or otherwise walling off the privileged information . . . suffice[s] to protect the state secrets and the case will proceed accordingly, with no consequences save those resulting from the loss of evidence." *Jeppesen*, 614 F.3d at 1082 (internal quotation marks and citation omitted). In *Reynolds*, for example, the Supreme Court concluded that an Air Force report sought during discovery was privileged and remanded the case to the district court to allow the plaintiffs to establish their claims without the privileged report. *See* 345 U.S. at 10-12. As with other evidentiary privileges, an opposing party remains free to seek nonprivileged evidence or go forward based on accessible information. *See Zubaydah*, 595 U.S. at 255-56 (Gorsuch, J., dissenting); *see also* 5 C. Wright & A. Miller, Federal Practice and Procedure § 1280 (4th ed. 2023) (privilege against self-incrimination); 3 Weinstein's Federal Evidence § 511.05 (attorney-client privilege).

In this case, however, the government maintains that protecting state secrets requires dismissing Fazaga's religion claims outright rather than just excluding the privileged information. The government invokes two of the "exceptional circumstances" which this court in *Jeppesen* recognized as requiring dismissal rather than just excluding evidence when the *Reynolds* privilege is properly invoked.[8] *Jeppesen*, 614 F.3d at 1077; *Fazaga*, 965 F.3d at 1041. The first exceptional circumstance is

---

[8] A third exceptional circumstance—if "the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence," *Jeppesen*, 614 F.3d at 1083 (quoting *Kasza*, 133 F.3d at 1166)—is not at issue in this case. Fazaga maintains that he can establish his *prima facie* case without privileged evidence.

"if the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim." *Jeppesen*, 614 F.3d at 1083 (quoting *Kasza*, 133 F.3d at 1166); *see also In re Sealed Case*, 494 F.3d 139, 149 (D.C. Cir. 2007); *Tenenbaum v. Simonini*, 372 F.3d 776, 777 (6th Cir. 2004); *Zuckerbraun v. Gen. Dynamics Corp.*, 935 F.2d 544, 547 (2d Cir. 1991). The second is if it is "impossible to proceed with the litigation because—privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses—litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Jeppesen*, 614 F.3d at 1083; *see also Sakab Saudi Holding Co. v. Aljabri*, 58 F.4th 585, 597 (1st Cir. 2023); *Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv.*, 14 F.4th 276, 303 (4th Cir. 2021).[9]

a.

Fazaga's primary response to the government's invocation of the *Jeppesen* exceptions is that *Jeppesen* is "clearly irreconcilable" with the Supreme Court's sub-

---

[9] We previously noted that the "modern state secrets doctrine," including both the *Totten* bar and the *Reynolds* privilege, is "[c]reated by federal common law." *Fazaga*, 965 F.3d at 1041. The *Reynolds* court noted that the existence of a "privilege against revealing military secrets" was "well established in the law of evidence," looking to both American and English historical precedent. 345 U.S. at 6-7. But the *effect* of the privilege in *Reynolds*—that the privileged evidence could not be compelled—was created by the Federal Rules of Civil Procedure, which exempt privileged material from disclosure. Outright dismissal, by contrast—whether because the entire subject matter of a case is a state secret as in *Totten* or because the case cannot be litigated without unacceptable risk of disclosing privileged material—is a remedy not provided by rule or statute and was created entirely as a matter of federal common law.

sequent decision in *General Dynamics Corp. v. United States*. After *General Dynamics*, Fazaga maintains, the invocation of the *Reynolds* evidentiary privilege results in the dismissal of a claim at the pleading stage only if the plaintiff cannot make a *prima facie* case without the privileged evidence.[10] *See Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). We do not agree that *Jeppesen* and *General Dynamics* are at odds in this respect.

General Dynamics involved a contract dispute between the Navy and two aerospace companies. 563 U.S. at 480-81. The parties disagreed about how application of the state secrets privilege under *Reynolds* should affect the case. *Id.* at 485. Noting that "*Reynolds* has less to do with these cases than the parties believe," the Supreme Court dismissed the case under the *Totten* bar. *Id.* at 485, 489-90. In reasoning that *Totten* applied, *General Dynamics* differentiated between the "common-law authority to fashion contractual remedies in Government-contracting disputes" under *Totten*, and the "power to determine the procedural rules of evidence" under *Reynolds*. *Id.* at 485. The Court also stated that, because the *Reynolds* privilege concerns evidentiary rules, "[t]he privileged information is excluded and the trial goes on without it." *Id.*

---

[10] The government asserts that Fazaga forfeited the argument that *Jeppesen* has been abrogated because the argument was not raised in the original briefing on appeal. But Plaintiffs raised and argued this same issue before the Supreme Court, which expressly reserved it, *see Fazaga*, 595 U.S. at 357, and it has been fully addressed in the parties' supplemental briefs before us now. As there is no prejudice to the defendants, we are comfortable addressing this purely legal issue on its merits. *See In re Mercury Interactive Corp. Sec. Litig.*, 618 F.3d 988, 992 (9th Cir. 2010).

Like *General Dynamics*, *Jeppesen* had explained that the dismissal that results from *Totten*'s justiciability bar is distinct from the consequences of the *Reynolds* evidentiary rule. 614 F.3d at 1087 n.12. So the two cases are the same in this regard. Because the dispute in *General Dynamics* was not resolved under *Reynolds*, the Supreme Court did not go on to address whether and in what circumstances the invocation of the *Reynolds* privilege justifies dismissing a case entirely. *Jeppesen* did address that question, before *General Dynamics* was decided. And in this case, decided after *General Dynamics*, the Supreme Court expressly declined to "delineate the circumstances in which dismissal is appropriate" or "determine whether dismissal was proper in this case" under the *Reynolds* privilege. *Fazaga*, 595 U.S. at 357. In other words, the Court recognized that the availability of dismissal as a remedy where the *Reynolds* privilege applies is an open question at the Supreme Court level.

The upshot is that *General Dynamics*' recognition that *Reynolds* applied an evidentiary rule does not contradict *Jeppesen*'s instruction that in certain "rare" circumstances, the invocation of the *Reynolds* evidentiary privilege may lead to dismissal. *Jeppesen*, 614 F.3d at 1092. The *General Dynamics* declaration thus did not wash out our own decision on that issue in *Jeppesen*, and *Jeppesen*'s parameters for dismissal under *Reynolds* remain binding in this circuit.

b.

Proceeding, then, to the question whether dismissal at the pleading stage was appropriate in this case, we begin with some background principles. We have made clear that "it should be a rare case" in which the *Reynolds* evidentiary privilege leads to dismissal—especially

"at the outset of a case." *Jeppesen*, 614 F.3d at 1092. "Dismissal at the pleading stage under *Reynolds* is a drastic result and should not be readily granted." *Id.* at 1089.

These cautions reflect that ordinarily, an evidentiary privilege is invoked to prevent the disclosure of *specific* evidence sought in discovery. *Reynolds*, for example, involved an assertion of the state secrets privilege over a particular government report alleged to contain state secrets. 345 U.S. at 3-4. Similarly, *Zubaydah* involved an assertion of the privilege to quash subpoenas to two former contractors requesting thirteen specific categories of documents related to a Central Intelligence Agency detention facility in Poland and to Zubaydah's treatment there. *See* 595 U.S. at 198-99. When the government asserts its state secrets privilege over particular evidence sought in discovery, the need for the assertion and its impact on the parties can be concretely evaluated and refined through discovery processes that serve to narrow and clarify the evidentiary issues in dispute between the parties. *See Hickman v. Taylor*, 329 U.S. 495, 501 (1947); *see also* 5 C. Wright & A. Miller, Federal Practice and Procedure §§ 1202, 1261 (4th ed. 2023). This "detailed *Reynolds* analysis," focused on specific evidence, helps to "ensure that the [state secrets] privilege is invoked no more . . . extensively than necessary" and to "improve the accuracy, transparency, and legitimacy of the proceedings." *Jeppesen*, 614 F.3d at 1080, 1084.

At the pleading stage, in contrast, any invocation of secrecy is necessarily broad and hypothetical. The plaintiff has not had an opportunity to pursue her theory of the case and so has not determined what specific evidence

she needs for it to succeed. The defendant also likely does not yet know in detail the defense to be asserted nor the evidence that will need to be relied on to support the defenses chosen. Dismissal at this preliminary stage travels far afield from the ordinary principles of evidentiary privilege and risks unnecessarily compromising access to the courts and foreclosing meritorious claims.

So, when the government seeks early dismissal based on the *Reynolds* privilege, we conduct a "searching examination," *Jeppesen*, 614 F.3d at 1092, with "a very careful, indeed a skeptical, eye," *Al-Haramain*, 507 F.3d at 1203, before concluding that dismissal is required. This inquiry does not detract from our firm "acknowledge[ment] [of] the need to defer to the Executive on matters of foreign policy and national security and surely [not] find ourselves second guessing the Executive in this arena." *Al-Haramain*, 507 F.3d at 1203. At the same time, the court's duty to "decide for itself whether the occasion is appropriate for claiming the privilege," *Zubaydah*, 595 U.S. at 205, is of paramount importance when the consequence of recognizing the privilege is outright dismissal at the pleading stage of a possibly meritorious lawsuit.

* * *

Here, after reviewing the government's classified materials *ex parte* and *in camera*, the district court dismissed Fazaga's claims under *Reynolds* and *Jeppesen* because (i) "privileged information gives Defendants a valid defense," and (ii) litigation "would present an unacceptable risk of disclosing state secrets." We address each rationale for dismissal in turn.

2.

One of the "exceptional circumstances" in which the *Reynolds* privilege can require dismissing a claim is if the state secrets privilege "deprives the defendant of information that would otherwise give the defendant a valid defense to the claim." *Jeppesen*, 614 F.3d at 1083 (quoting *Kasza*, 133 F.3d at 1166). We first address the proper standard and procedures for concluding that privileged information establishes a valid defense that requires dismissal, which the parties dispute, and then consider whether that standard has been met in this case.

a.

Although *Jeppesen* briefly restated the "valid defense" ground for dismissal, it did not dismiss any claims on that basis and so did not elaborate on the standard for doing so.[11] We addressed the "valid defense" standard in some detail in our earlier opinion in this case, adopting the D.C. Circuit's approach as set forth in *In re Sealed Case*, 494 F.3d at 149, and explaining that a "valid defense" is one that "is meritorious and not merely plausible and would *require* judgment for the de-

---

[11] None of the cases to which *Jeppesen*'s "valid defense" language can be traced actually applied the stated rule that "if the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant." *Jeppesen*, 614 F.3d at 1083 (quoting *Kasza*, 133 F.3d at 1166). *Jeppesen* quoted this language from *Kasza*, which similarly stated but did not apply the rule. *See Kasza*, 133 F.3d at 1166, 1170. *Kasza* quoted this language from *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992). But the *Bareford* language was not a holding: *Bareford* recognized but expressly declined to adopt other courts' conclusions that dismissal was warranted "if privileged information would establish a valid defense." *Id.* at 1143.

fendant," *Fazaga*, 965 F.3d at 1067 (emphasis added). Addressing the implementation of this concept, we explained that "where the government contends that dismissal is required because the state secrets privilege inhibits it from presenting a valid defense, the district court may properly dismiss the complaint only if it conducts an 'appropriately tailored *in camera* review of the privileged record,' and determines that defendants have a legally meritorious defense that prevents recovery by the plaintiffs." *Fazaga*, 965 F.3d at 1067 (citation omitted) (quoting *In re Sealed Case*, 494 F.3d at 151).

We discussed the meaning of "valid defense" in our earlier opinion because we recognized that the district court might need to evaluate privilege claims involving information not covered by FISA's alternate procedure (as we interpreted it) to determine whether dismissal was required under *Jeppesen*. *Fazaga*, 965 F.3d at 1067. The Supreme Court reversed our resolution under FISA of the state secrets challenge but did not address our articulation of the valid defense standard. *Fazaga*, 595 U.S. at 357-59.

Contrary to the government's argument, our definition of "valid defense" in our earlier opinion in this case was not dicta and remains circuit law. "Where a panel confronts an issue germane to the eventual resolution of the case, and resolves it after reasoned consideration in a published opinion, that ruling becomes the law of the circuit, regardless of whether doing so is necessary in some strict logical sense." *United States v. McAdory*, 935 F.3d 838, 843 (9th Cir. 2019) (quoting *Cetacean Cmty. v. Bush*, 386 F.3d 1169, 1173 (9th Cir. 2004)). In particular, "direction to the district court on how to proceed continues to be binding precedent." *California*

Pro-Life Council, Inc. v. Randolph, 507 F.3d 1172, 1176 (9th Cir. 2007) (quoting *Operating Eng'rs Pension Tr. v. Charles Minor Equip. Rental, Inc.*, 766 F.2d 1301, 1304 (9th Cir. 1985)). Regardless of whether it was "in some technical sense 'necessary,'" our definition of "valid defense" was intended to govern this case as it went forward, and so is the "law of the circuit." *See Barapind v. Enomoto*, 400 F.3d 744, 751 (9th Cir. 2005) (en banc) (per curiam).[12]

In any event, we remain of the view that our earlier explanation of the "valid defense" ground for dismissal was correct.[13] To see why, we begin by outlining the rationales for sanctioning dismissals in rare circumstances when the state secrets privilege is invoked by a government defendant, and then explain why those rationales do not justify expanding the exception to defenses that may be meritorious but may not be.

---

[12] We reject the government's invocation of the "clear error" exception to the *law of the case* doctrine. "[E]xceptions to the law of the case doctrine are not exceptions to our general 'law of the circuit.'" *Gonzalez v. Arizona*, 677 F.3d 383, 389 n.4 (9th Cir. 2012) (en banc). As we have explained, our explanation of "valid defense" is circuit law that "must be followed unless and until overruled." *Hart v. Massanari*, 266 F.3d 1155, 1170 (9th Cir. 2001).

[13] None of the cases the government cites in arguing that our "valid defense" standard is foreclosed substantively addressed that ground for dismissal or dismissed a claim on this basis. *See Reynolds*, 345 U.S. at 11 (remand); *Jeppesen*, 614 F.3d at 1087 (dismissal "because there is no feasible way to litigate . . . without creating an unjustifiable risk of divulging state secrets"); *Gen. Dynamics*, 563 U.S. at 486-89 (*Totten* dismissal); *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005) (dismissal where "object of the suit . . . is to establish a fact that is a state secret"); *El-Masri v. United States*, 479 F.3d 296, 308-10 (4th Cir. 2007) (dismissal where privileged evidence necessary to the plaintiff's *prima facie* case).

First, to repeat, dismissal because privileged information supports a valid defense turns the normal principles of evidentiary privilege on their head; normally, "privileged information is excluded and the trial goes on." *Gen. Dynamics*, 563 U.S. at 485. But most evidentiary privileges, like the attorney-client privilege or the marital privilege, protect *private* interests, either of the litigants themselves or of other people. In such instances, if a claim or defense depends on privileged information, the privilege holder "has a choice" between waiving the privilege to pursue the claim or defense and waiving the claim or defense to keep the privileged information confidential. *United States v. Gonzalez*, 669 F.3d 974, 982 (9th Cir. 2012). For evidentiary privileges that protect private interests, allowing the privilege holders to decide for themselves whether to forfeit a claim or defense so as to keep the privileged information private suffices; there is no need for the court to decide whether the case should go forward despite the privilege invocation.

The state secrets privilege is different. It protects a *public* interest in safeguarding information that, if disclosed, would harm the nation's defense, intelligence-gathering, or foreign-relations interests. So the dangers of proceeding with the case may transcend the impairment of the government's private interest in defending the litigation; that interest, standing alone, might counsel waiving any privilege so as to enhance the defense. The "valid defense" ground for dismissal absolves the government, in the interest of national security, from having to choose between waiving the state secrets privilege to assert a defense and keeping the

privileged materials private by abandoning any defense that relies on them.[14]

Second, a related reason the valid defense ground for dismissal has been justified is to protect the integrity of the judicial process. In *Molerio v. FBI*, for example, the plaintiff alleged that the FBI had decided not to hire him because of his father's political activities. 749 F.2d 815, 818-20 (D.C. Cir. 1984). The D.C. Circuit concluded that the plaintiff had made out a "circumstantial case" that the FBI had violated the First Amendment because the political activities were a substantial or motivating factor in the FBI's failure to hire the plaintiff. *Id.* at 825. But the court had reviewed a privileged submission from the government *ex parte* and *in camera*. *Id.* As a result of that review, "the court [knew] that the reason [the plaintiff] was not hired had nothing to do with [his father's] assertion of First Amendment rights." *Id.* The court recognized that if the privileged information were excluded as required under *Reynolds*, "there may be enough circumstantial evidence to permit a jury to come to [the] erroneous conclusion" that the reason the FBI didn't hire Molerio was his father's protected speech. *Id.* The court in *Molerio* specifically distinguished the situation before it from that in *Ellsberg v. Mitchell*, where the court's review of the privileged information "*did not*

[14] There is an analogous tension in cases involving claims against individual defendants. *Ellsberg v. Mitchell*, for example, discussed how officials sued in their individual capacities could be "trapped by the government's assertion of its state secrets privilege" in cases where excluding privileged information "[d]eprived [them] of the ability in practice to adduce the evidence necessary to mount a defense to the plaintiffs' *prima facie* case." 709 F.2d 51, 69-70 (D.C. Cir. 1983). The valid defense ground for dismissal mitigates this risk as well.

ipso facto disclose to the court the validity of the defense." *Id.* (emphasis added). As the *Molerio* court "kn[ew] that further activity in this case would involve an attempt . . . to convince the jury of a falsehood," it concluded that "it would be a mockery of justice for the court—knowing the erroneousness—to participate in that exercise." *Id.*

Crucially, these rationales for the "valid defense" ground for dismissal are not linked to the generalized risk that privileged information might be disclosed if the litigation moves forward. That concern is instead analyzed and protected under the rubric of *Jeppesen*'s unacceptable-risk-of-disclosure dismissal ground. Rather, the "valid defense" ground protects against the unfairness that would result if there exists evidence that is factually and legally sufficient to establish an actually meritorious defense but cannot be introduced without endangering national security.

With that background, we reiterate that a valid-defense dismissal is warranted only if the privileged information establishes that the defense is legally meritorious and would require judgment against the plaintiff. In other words, the privileged information must establish a legally and factually valid defense. Any lesser standard could foreclose potentially meritorious claims based on conjecture and so would go beyond protecting defendants from any unfairness caused by protecting state secrets and the court from ratifying a result it knows to be incorrect. "Just as it would be manifestly unfair to permit a presumption of unconstitutional conduct to run against the defendant when the privilege is invoked, it would be manifestly unfair to a plaintiff to impose a presumption that the defendant has a valid de-

fense that is obscured by the privilege." *In re Sealed Case*, 494 F.3d at 150 (internal quotation marks, alterations, and citation omitted).

We note as well that there is a risk that the state secrets privilege can be invoked not to protect the public interest in national security but to shield the government from embarrassment or unwanted scrutiny. In *Reynolds*, for example, courts allowed the government to invoke the state secrets privilege to withhold the report plaintiffs had requested, doing so "without even pausing to review the report independently in chambers or asking a lower court to take up that task." *Zubaydah*, 595 U.S. at 251 (Gorsuch, J., dissenting). Decades later, the report was declassified and was revealed to detail the Air Force's negligence rather than state secrets. *See* Louis Fisher, *In the Name of National Security: Unchecked Presidential Power and the* Reynolds *Case* 165-69 (2006). *Reynolds*—and, with it, the modern state secrets doctrine—was thus based on the government's misrepresentation in court that the report contained secret information. *See id.* at 193; *Zubaydah*, 595 U.S. at 251 (Gorsuch, J., dissenting).

We stress that we have no reason whatever to think that the government here is misleading this court. But the inherent tension when the government is both a litigating party and the caretaker of national security secrets further cautions against dismissing a potentially viable lawsuit. As with conflicts of interest generally, the problem is not that the litigant or its attorney will consciously claim a privilege or make representations that prove to be unjustified or exaggerated. The problem is rather that the competing pressures will lead to unacknowledged and unintentional compromises of the

countervailing interest in court access for potentially meritorious cases, especially cases like this one charging violations of constitutional rights. Given this tension—and without suggesting that the government actors in this case or any other are not proceeding with the utmost good faith in their state secrets assertions—courts are obliged to scrutinize independently the government's invocations of the state secrets privilege, and to do so at the appropriate stage of the litigation and with sufficiently detailed support, rather than accepting them at the outset and at face value.

For these reasons, it is not enough to articulate a *potentially* valid defense, or to suggest that mounting a defense *might* require privileged evidence. Put another way, if the defense would *in fact* fail, there would be no prejudice to a government defendant from excluding the privileged evidence and allowing the case to proceed, nor any sense in which the courts were sanctioning an unfair result.

b.

That conclusion raises the question how courts are to determine whether privileged information establishes "a legally meritorious defense that prevents recovery by the plaintiffs." *Fazaga*, 965 F.3d at 1067. The inquiry is necessarily a factual one. The district court must make "factual judgments," *Ellsberg*, 709 F.2d at 69, and consider potentially disputed issues of material fact, *see Molerio*, 749 F.2d at 824. Because this inquiry focuses on potential *defenses* and other material beyond the pleadings rather than just the allegations of the complaint, valid-defense dismissal is not ordinarily appropriate under Rule 12(b)(6). As *Jeppesen* observed, "*Reynolds* necessarily entails consideration of materials

outside the pleadings. . . . That fact alone calls into question reliance on Rule 12(b)(6)." 614 F.3d at 1093 n.16.

So, if dismissal based on a valid defense usually cannot be granted under Rule 12(b)(6), what process is appropriate for a court to use to determine whether privileged information establishes a legally meritorious defense? In *Jeppesen*, we stated that "if the [*Reynolds*] privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant *summary judgment* to the defendant." 614 F.3d at 1083 (quoting *Kasza,* 133 F.3d at 1166) (emphasis added). But the Rule 56 summary judgment standard is not a perfect fit for this determination either. *See Molerio*, 749 F.2d at 824. After all, the *ex parte* nature of a court's review of privileged submissions means that the plaintiff will not have the chance to "dispute . . . material fact[s]." *See* Fed. R. Civ. P. 56(a).

Still, even if not in technical compliance with Rule 56, the practicalities of the situation counsel that both sides must be given an opportunity to offer evidence supporting their positions concerning whether the proffered defense is valid before a court can dismiss a claim because privileged information establishes a valid defense. The invocation of a defense premised on assertedly privileged material, combined with a request to dismiss the case so as to protect the privileged material, can only be fairly evaluated if the district court itself reviews the defendant's evidence, *in camera* and *ex parte* to the extent the material is covered by the assertion of the state secrets privilege; concomitantly, the plaintiff must be given the opportunity to submit actual evidence to prove up a

prima facie case and refute the defense. Unlike in a typical summary judgment, the task of evaluating each party's evidence and resolving any disputes or inconsistencies to determine whether the defendant has a meritorious defense necessarily falls on the court. But the unusual nature of this procedure and the lack of transparency built into it is the price of protecting the defendant's ability to mount a defense without exposing state secrets while preserving for the plaintiffs both court access and the ability meaningfully to litigate their case to the extent feasible.[15]

When the government seeks only to exclude privileged information, it can sometimes invoke the *Reynolds* privilege without making "a complete disclosure," and a court need not "insist[] upon an examination of the evidence." *Reynolds*, 345 U.S. at 10. But to justify dismissing a claim outright rather than simply excluding privileged information, the government must be prepared to disclose to the court the specific information that establishes its defense. The form and specificity of the government's submission will of course depend on "the circumstances of the case" and the nature of the information. *See id.* But the submission must be detailed enough to make "clear" to the reviewing court that "dismissal is *required*" because the privileged information

[15] Our holding that the valid defense ground for dismissal ordinarily cannot be resolved at the pleading stage under Rule 12 does not mean that plaintiffs will be allowed to seek discovery of privileged information. The Federal Rules exclude privileged material from the scope of discovery. Fed. R. Civ. P. 26(b)(1). And *Jeppesen*'s unacceptable-risk-of-disclosure dismissal ground protects against the risk that the process of discovery could itself disclose privileged information.

clearly shows the defendant's entitlement to judgment. *Jeppesen*, 614 F.3d at 1089 (emphasis added).

We recognize that the procedure we envision is unorthodox, as it melds summary judgment procedures with an expanded, nontransparent factfinding role for judges. But the alternative is also unorthodox: closing the courthouse door to potentially meritorious lawsuits because of a defense that may or may not be viable once examined. Faced with that dilemma, the procedure we have described is the best option.

c.

We now consider whether Fazaga's claims must be dismissed at this juncture because privileged information establishes a valid defense. We conclude that, although at least some of the information at issue is privileged, the district court did not apply the standard we have enunciated, or use the process we have described, when it decided that the case should be dismissed because the government has a "valid defense."

The district court stated tersely at the outset of its valid defense analysis that "the privileged information gives [the government] a valid defense." But in explaining its valid defense ruling, the district court reasoned only that the defenses the government would try to mount against Fazaga's various claims would all need to rely in part on privileged information. The court noted that defending against the discrimination claims would require the government to demonstrate that its investigations "were properly predicated and focused," which would "require" the government "to summon privileged evidence related to Operation Flex." Similarly, the district court explained that the government could defend against Fazaga's First Amendment claims by demon-

strating that its actions were narrowly tailored to achieve a compelling government interest—questions the district court noted were "fact intensive" and would "necessitate a detailed inquiry into the nature, scope, and reasons for the investigations under Operation Flex." Finally, the district court stated that the government "may have a valid defense" against Fazaga's FTCA claim under the discretionary-function exception, but stated that establishing such a defense would require the government to "marshal facts that fall within the three privileged categories of information related to Operation Flex."

This summary demonstrates that the district court did not conduct the factual review required to conclude that Fazaga's claims must be dismissed on the valid defense ground. As we have explained, the government is not entitled to dismissal simply because it *may* assert a defense that *could* require introducing privileged information. The district court's analysis here went only that far: The court speculated that defending against Fazaga's claims *could* require the government to "marshal" privileged information and would necessitate a "fact-intensive" and "detailed inquiry" into Operation Flex. But the district court dismissed Fazaga's claims because such an inquiry into privileged information would be eventually required; it did not conduct that inquiry and conclude that the privileged information submitted established a defense that is "meritorious and not merely plausible," such that it "would *require* judgment for the defendant." *Fazaga*, 965 F.3d at 1067 (quoting *In re Sealed Case*, 494 F.3d at 149) (emphasis added).

In addition, the district court did not give Fazaga an opportunity to submit evidence to prove up his *prima*

facie case, as we have held is required. Fazaga maintains that he can build such a case based on publicly available and nonprivileged evidence about Monteilh's activities and the information he gathered, without any discovery.[16] Fazaga might well, for example, be able to offer nonprivileged evidence from Monteilh, a percipient witness, regarding the government's surveillance instructions. The district court, however, weighed the government's evidentiary submissions against Fazaga's *allegations*, without giving him a parallel opportunity to provide actual evidence. As we have explained, a court may not "grant summary judgment to the defendant" on the basis that the state secrets "privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim," *Jeppesen*, 614 F.3d at 1083, without considering factual submissions from each party.

In sum, the district court has not yet conducted the detailed and fact-intensive inquiry required to dismiss a claim based on a valid defense under *Reynolds*. We cannot sustain its dismissal of Fazaga's religion claims on the "valid defense" ground.

We therefore remand this case so that the district court can undertake the factual inquiry required to de-

---

[16] Fazaga goes on to suggest that if the government provides evidence, in court or *in camera*, to rebut the *prima facie* claim, "extremely limited discovery" into information that Fazaga maintains is not privileged would be sufficient to resolve the issue. As we explain later, *infra* p. 44-45 and note 20, the government has indicated that considerably more unprivileged material will be available on remand than previously, including with regard to the instructions Monteilh received. The result may be that Fazaga will not request even "extremely limited discovery." We comment later on the appropriate approach if he does. *See infra* p. 46.

termine whether dismissal based on a valid defense is warranted. On remand, the district court should provide Fazaga an opportunity to prove his *prima facie* case without privileged information. The government should have the chance to show that specific privileged information establishes a valid defense.[17] The district court will be able to review the privileged information *in camera* and consider, based on the submissions from each party, whether the privileged information establishes a valid defense and so requires dismissing Fazaga's claims.

3.

Another "exceptional circumstance" in which the *Reynolds* privilege can require dismissing a claim is if the privileged information is so "inseparable from nonprivileged information that will be necessary to the claims or defenses" that "litigating the case . . . would present an unacceptable risk of disclosing state secrets." *Jeppesen*, 614 F.3d at 1083. The district court's dismissal of Fazaga's claims on this basis does not meet the stringent standard for such dismissals.

"[W]henever possible, sensitive information must be disentangled from nonsensitive information to allow for

---

[17] If the government's prior submissions (which summarize but do not actually include the underlying classified source material) are not detailed and reliable enough to support this inquiry, the district court can request a more robust record. If the submissions are detailed and reliable enough, the district court can carefully consider *which* of the government's evidentiary submissions is (i) privileged, and (ii) necessary to prove a valid defense. If the valid defense can be proven without privileged information, dismissal is not warranted; if only some of the information is privileged, the unprivileged material relied upon should be provided to the plaintiffs, as in an ordinary summary judgment proceeding (subject to the other *Jeppesen* ground for dismissal, discussed next).

the release of the latter." *Kasza*, 133 F.3d at 1166 (quoting *Ellsberg*, 709 F.2d at 57). District courts generally "are well equipped to wall off isolated secrets from disclosure." *Jeppesen*, 614 F.3d at 1089. But in certain "exceptional cases," the secret information may be "impossible to isolate and even efforts to define a boundary between privileged and unprivileged evidence would risk disclosure by implication." *Id.* In those cases, a court may "restrict the parties' access not only to evidence which itself risks the disclosure of a state secret, but also those pieces of evidence or areas of questioning which press so closely upon highly sensitive material that they create a high risk of inadvertent or indirect disclosures." *Id.* at 1082 (quoting *Bareford v. Gen. Dynamics Corp.*, 973 F.2d 1138, 1143-44 (5th Cir. 1992)). In the rare instance in which the risk of disclosure cannot be averted through the protective measures routinely used by courts, the case must be dismissed, leaving the plaintiff without a remedy for a possibly meritorious claim. The government here has not at this stage established "either a certainty or an unacceptable risk" that proceeding with litigation will reveal state secrets. *Jeppesen*, 614 F.3d at 1087-88 n.12.

Fazaga's core allegation is that the defendants improperly targeted Fazaga and other Muslims because of their religion. The government argues that "[t]here is no way to litigate that core allegation without examining state secrets: the government's actual reasons for conducting the FBI counterterrorism investigations at issue here and the nature and scope of those investigations." But, in the unique posture of this case, it is, for several reasons, not apparent at the pleading stage that "the facts underlying plaintiffs' claims are so infused with these secrets" that this litigation cannot proceed

with appropriate protective measures in place. *See Jeppesen*, 614 F.3d at 1088.

First, the district court did not consider all of the potential protective measures or explain why they would not be sufficient to protect the privileged information if litigation were to proceed. The district court referred generally to "protective procedures available to the [c]ourt," specifically mentioning only "protective orders or restrictions on testimony." But district courts have other tools to handle sensitive information. Moreover, even those two mechanisms are broad categories, and the district court did not disaggregate them.

Various procedures that could allow this case to proceed further have been proposed during the course of this litigation. One is the possibility of the *ex parte* and *in camera* proceeding described above in which the government would furnish privileged source material, and the district court could then determine whether the government has a valid defense based on its review of the underlying information.

There are other options, too. Federal courts have long used *in camera* review, protective orders, and other procedures to enable judges to review sensitive information. Congress has codified some of these procedures for specific circumstances. For example, FISA contemplates *in camera*, *ex parte* review of extremely sensitive information, along with the use of protective orders to bind nongovernment parties. 50 U.S.C. § 1806(f). The Classified Information Procedures Act allows courts to permit "statement[s] admitting relevant facts that the specific classified information would tend to prove" or "a summary of the specific classified information" to substitute for classified information. 18 U.S.C. App. § 6(c)(1).

The district court might also consider appointing a special master with a security clearance to examine the assertedly privileged material. That master could (i) curate for the court a representative sample of the classified documents and (ii) summarize specific legal arguments each party could make based on the classified information, especially possible defenses. *See In re U.S. Dep't of Def.*, 848 F.2d 232, 234, 236 (D.C. Cir. 1988); *see also* Fed. R. Civ. P. 53(a)(1)(B)(i).[18] Alternatively, the government (or a neutral third party) could reformat the most sensitive privileged material—for example by providing the court classified documents with targeted redactions.[19]

Second, the unusual circumstances of this case particularly counsel against early dismissal. Those circumstances are these: The government revealed Monteilh's role as a confidential informant in an unrelated criminal case. It also recognizes that there is substantial relevant nonprivileged evidence that could be (and to a degree has been) disclosed in this litigation. Monteilh has provided extensive nonclassified declarations discussing his role in Operation Flex and his interactions with Fazaga and others, and some of the recordings from Monteilh's informant work are now public.[20] The gov-

---

[18] A special master with a security clearance may be an efficient way to review a large body of classified material, given the logistical difficulties of clearing term judicial law clerks. *See In re Dep't of Def.*, 848 F.2d at 236, 238-39.

[19] If the dismissal issue arises again in this case, the district court should consider these alternatives, and others that may be suggested, to determine after a careful, detailed inquiry whether there is a real and unmitigable risk that privileged information could be revealed if the case proceeds.

[20] The government informed the court in a letter after oral argument that the FBI has reviewed the audio and video collected by

ernment has informed us that it "expects that, on remand, it will be able to . . . make the substantial majority of the audio and video [collected by Monteilh] available for further proceedings, subject to an appropriate Privacy Act protective order" and redactions. The government's recognition that circumstances have changed to some degree suggests that the district court's generalized assessment should be replaced by individualized consideration of the need for specific pieces of defensive evidence after Fazaga has the chance to present an evidence-based *prima facie* case and sharpen the issues that remain.

Further, Fazaga emphasized that he does not "need any discovery into the secret evidence" and "disclaim[ed] any need for it." As noted, Fazaga maintains that he can build a *prima facie* case based on nonprivileged evidence about Monteilh's activities and without any discovery. *See supra* p. 40 and note 16. The government defendants *may* be able to defend against those claims without relying on privileged information—by, for example, demonstrating on the evidence Fazaga presents that there was a compelling reason for investigating these individuals and no less restrictive alternative, or that the challenged conduct falls within the FTCA's discretionary function exception.

Third, the government's assertion that *any* further litigation poses an unacceptable risk of disclosure is un-

---

Mr. Monteilh and, as the FBI previously expected, the FBI has determined that the substantial majority of the audio and video will be available for further proceedings in this case. The FBI has made preliminary redactions and expects that, on remand, it will be able to make the substantial majority of the audio and video at issue available, subject to an appropriate Privacy Act protective order.

dercut by the detailed classified disclosures it has already presented to the district court, our court, and the Supreme Court. This case has proceeded for more than a decade without any classified or privileged information being made public. We therefore hesitate to credit vague fears that unspecified classified information could be revealed if the case goes forward, rather than allowing this case to proceed to the point where it is possible to focus on the need to protect specific pieces of information. To justify dismissal, the government would have to specify why, even though state secrets have so far in this case been communicated *ex parte* and *in camera* to three levels of court without issue, there remains a danger that particular privileged information will be disclosed if proceedings continue.

We emphasize that if the case is to proceed, discovery, if any, will need to be extremely limited and closely monitored to avoid disclosing privileged information. The government appears to have acknowledged earlier in the case that, with such monitoring, further proceedings are possible. In its motion to dismiss, the government suggested that, "[t]o the extent that the Court wishes to assess the impact of the privilege assertion as to claims against the Government Defendants, it should require plaintiffs to proffer in proceedings under Rules 16 and 26 precisely what discovery it intends to seek against the Government" and allow the government to assert the privilege at that point. The government has not heretofore shown that such protective measures would not sufficiently reduce the risk of disclosing secret information in the future.

The "broad sweep" of the state secrets privilege "requires that the privilege not be used to shield any mate-

rial not strictly necessary to prevent injury to national security and counsels that whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter." *In re United States*, 872 F.2d 472, 476 (D.C. Cir. 1989) (internal citations and quotation marks omitted). We are not convinced that the significant amount of nonprivileged information in this case, including information that will be newly available on remand, cannot be disentangled from privileged national security secrets. If it does become clear that the court cannot disentangle nonprivileged information that is necessary for its case from privileged information, the government will remain free to seek dismissal; the district court will then evaluate the government's request based on the specific information then available.

We conclude that the dismissal was not appropriate at this stage. The district court can determine on remand what safeguards are required to protect privileged information as the case goes forward; and, if asked to do so, reconsider a dismissal request based on new developments in the case.

IV.

We close our state secrets privilege discussion with two observations and some further reflections.

First, more than thirteen years have passed since the government first asserted the state secrets privilege in this case. Since then, new revelations have informed the public about increasingly bygone government actions. Ten additional people have served as Attorney General. It is far from certain that every piece of information over which the government asserted the state secrets privilege in 2011 need remain secret today. And pieces of in-

formation that remain privileged may now be easier to disentangle from non-secret information. The government has made clear that its approach to classification is, commendably, dynamic. The upshot is that much more information might now be made available either to Fazaga or, if necessary, *in camera* to the court, without endangering national security.

Second, we are convinced that there are concrete possibilities for proceeding in this case. We remand with the expectation that the district court will consider the viability of procedures that will enable this litigation to move forward and facilitate some degree of interaction with the underlying source material, perhaps with the benefit of additional briefing by the parties as to such means. Again, any discovery will need to be closely monitored. But as we have said, we are not convinced that the full panoply of measures that could protect secret information has yet been exhausted. We leave it to the district court to employ the appropriate tools both to evaluate particularized invocations of state secrecy under *Reynolds* and to ensure that privileged information is appropriately handled.

The national security concerns in this case are serious. If it becomes evident that this case cannot be litigated without endangering national security, Fazaga's private interest will have to yield. We emphasize that nothing in this opinion forecloses the government from asserting the privilege over specific pieces of evidence that become pertinent in the course of litigation, as the government did in *Reynolds* and *Zubaydah* and as it suggests it intends to do here, or from seeking dismissal because specific privileged evidence is essential to an articulated defense and cannot feasibly and safely be pre-

sented only *in camera*. But we emphasize as well that we should not cross that bridge until we have no choice but to do so. The record and disclosures before us at this early stage of litigation demonstrate that dismissal of Fazaga's claims at this juncture prematurely barred the courthouse door without assurance that there is no alternative to doing so.

CONCLUSION

For the foregoing reasons, we **DISMISS** the remaining *Bivens* claims. Because the grounds specified by the district court do not warrant dismissal of the religion claims at this juncture, we **REVERSE** and **REMAND** those claims to the district court, along with the FISA claims and the Fourth Amendment claims for injunctive relief that we held cognizable in our prior opinion, for further proceedings in accord with this opinion and, to the degree still applicable, the earlier one.

APPENDIX B

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 12-56867
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLEES

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; PAT ROSE;
KEVIN ARMSTRONG; PAUL ALLEN, DEFENDANTS

AND

BARBARA WALLS; J. STEPHEN TIDWELL,
DEFENDANTS-APPELLANTS

No. 12-56874
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLEES

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN

TIDWELL; BARBARA WALLS, DEFENDANTS

AND

PAT ROSE; KEVIN ARMSTRONG; PAUL ALLEN,
DEFENDANTS-APPELLANTS

No. 13-55017

D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELANTS

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN
TIDWELL; BARBARA WALLS; PAT ROSE; KEVIN
ARMSTRONG; PAUL ALLEN; UNITED STATES OF AMERICA,
DEFENDANTS-APPELLEES

Argued and Submitted: Dec. 7, 2015
Pasadena, California
Filed: Feb. 28, 2019
Amended: July 20, 2020

Appeal from the United States District Court
for the Central District of California
Cormac J. Carney, District Judge, Presiding

ORDER AND AMENDED OPINION

Before: RONALD M. GOULD AND MARSHA S. BERZON, CIRCUIT JUDGES and GEORGE CARAM STEEH III*, District Judge.

ORDER

The opinion filed on February 28, 2019, reported at 916 F.3d 1202, is hereby amended. An amended opinion is filed concurrently with this order. With these amendments, the panel has unanimously voted to deny appellees' petition for rehearing. Judges Berzon and Gould have voted to deny the petition for rehearing en banc and Judge Steeh so recommends.

The full court has been advised of the petition for rehearing en banc. A judge of the court requested a vote on en banc rehearing. The matter failed to receive a majority of votes of non-recused active judges in favor of en banc consideration. Fed. R. App. P. 35.

The petition for rehearing and the petition for rehearing en banc are **DENIED**. No further petitions for panel rehearing or rehearing en banc will be entertained. Judge Berzon's concurrence with and Judge Bumatay's dissent from denial of en banc rehearing are filed concurrently herewith.

---

* The Honorable George Caram Steeh III, United States District Judge for the Eastern District of Michigan, sitting by designation.

OPINION

TABLE OF CONTENTS

BERZON, Circuit Judge:

INTRODUCTION

Three Muslim residents of Southern California allege that, for more than a year, the Federal Bureau of Investigation ("FBI") paid a confidential informant to conduct a covert surveillance program that gathered information about Muslims based solely on their religious identity. The three plaintiffs filed a putative class action against the United States, the FBI, and two FBI officers in their official capacities ("Government" or "Government Defendants"), and against five FBI agents in their individual capacities ("Agent Defendants"). Alleging that the investigation involved unlawful searches and anti-Muslim

discrimination, they pleaded eleven constitutional and statutory causes of action.[1]

The Attorney General of the United States asserted the state secrets privilege with respect to three categories of evidence assertedly at issue in the case, and the Government moved to dismiss the discrimination claims pursuant to that privilege. The Government expressly did not move to dismiss the Fourth Amendment and Foreign Intelligence Surveillance Act ("FISA") unlawful search claims based on the privilege. Both the Government and the Agent Defendants additionally moved to dismiss Plaintiffs' discrimination and unlawful search claims based on arguments other than the privilege.

The district court dismissed all but one of Plaintiffs' claims on the basis of the state secrets privilege—including the Fourth Amendment claim, although the Government Defendants had not sought its dismissal on privilege grounds. The district court allowed only the FISA claim against the Agent Defendants to proceed. Plaintiffs appeal the dismissal of the majority of their claims, and the Agent Defendants appeal the denial of qualified immunity on the FISA claim.

We conclude that some of the claims dismissed on state secrets grounds should not have been dismissed outright. Instead, the district court should have reviewed any state secrets evidence necessary for a deter-

---

[1] Specifically, the Plaintiffs alleged violations of the First Amendment's Establishment Clause and Free Exercise Clauses; the Religious Freedom Restoration Act, 42 U.S.C. § 2000bb *et seq.*; the equal protection component of the Fifth Amendment's Due Process Clause; the Privacy Act, 5 U.S.C. § 552a; the Fourth Amendment; the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810; and the Federal Tort Claims Act, 28 U.S.C. § 1346.

mination of whether the alleged surveillance was unlawful following the secrecy-protective procedure set forth in FISA. *See* 50 U.S.C. § 1806(f). After addressing Defendants' other arguments for dismissing Plaintiffs' claims, we conclude that some of Plaintiffs' allegations state a claim while others do not. Accordingly, we remand to the district court for further proceedings on the substantively stated claims.

BACKGROUND

At this stage in the litigation, we "construe the complaint in the light most favorable to the plaintiff[s], taking all [their] allegations as true and drawing all reasonable inferences from the complaint in [their] favor." *Doe v. United States*, 419 F.3d 1058, 1062 (9th Cir. 2005). "Conclusory allegations and unreasonable inferences, however, are insufficient to defeat a motion to dismiss." *Sanders v. Brown*, 504 F.3d 903, 910 (9th Cir. 2007).

Plaintiffs are three Muslims who were residents of Southern California: Sheikh Yassir Fazaga, Ali Uddin Malik, and Yasser AbdelRahim. Fazaga was, at the times relevant to this litigation, an imam at the Orange County Islamic Foundation ("OCIF"), a mosque in Mission Viejo, California. Malik and AbdelRahim are practicing Muslims who regularly attended religious services at the Islamic Center of Irvine ("ICOI").

The complaint sought relief against the United States, the FBI, and two federal officials named in their official capacities, as well as five individual Agent Defendants—Kevin Armstrong, Paul Allen, J. Stephen Tidwell, Barbara Walls, and Pat Rose—named in their individual capacities. Armstrong and Allen were FBI Special Agents assigned to the Orange County areas; Tidwell was the Assistant Director in Charge of the FBI's Los Angeles

Field Office from August 2005 to December 2007; Walls was the Special Agent in Charge of the FBI's Santa Ana branch office, a satellite office of the FBI's Los Angeles field office; and Rose was a Special Agent assigned to the FBI's Santa Ana branch office.

Because of the sensitivity of the issues in this case, we particularly stress the usual admonition that accompanies judicial determination on motions to dismiss a complaint: the facts recited below come primarily from Plaintiffs' allegations in their complaint.[2] The substance of those allegations has not been directly addressed by the defendants. At this point in the litigation, the truth or falsity of the allegations therefore is entirely unproven.

I. Factual Background

For at least fourteen months in 2006 and 2007, the FBI paid a confidential informant named Craig Monteilh to gather information as part of a counterterrorism investigation known as Operation Flex. Plaintiffs allege that Operation Flex was a "dragnet surveillance" program, the "central feature" of which was to "gather information on Muslims."[3]

---

[2] In addition to the facts alleged in the complaint, this opinion at some points refers to facts contained in two public declarations submitted by the Government in support of its invocation of the state secrets privilege.

[3] In a public declaration, the FBI frames Operation Flex differently, contending that it "focused on fewer than 25 individuals and was directed at detecting and preventing possible terrorist attacks." The FBI maintains that the goal of Operation Flex "was to determine whether particular individuals were involved in the recruitment and training of individuals in the United States or overseas for possible terrorist activity."

At some point before July 2006, Stephen Tidwell, then the Assistant Director in Charge of the FBI's Los Angeles Field Office, authorized first the search for an informant and later the selection of Monteilh as that informant. Once selected, Monteilh was supervised by two FBI handlers, Special Agents Kevin Armstrong and Paul Allen.

In July 2006, Monteilh began attending ICOI. As instructed by Allen and Armstrong, Monteilh requested a meeting with ICOI's imam, represented that he wanted to convert to Islam, and later publicly declared his embrace of Islam at a prayer service. Monteilh subsequently adopted the name Farouk al-Aziz and began visiting ICOI daily, attending prayers, classes, and special events. He also visited "with some regularity" several other large mosques in Orange County.

Armstrong and Allen closely supervised Monteilh during the course of Operation Flex, explaining to him the parameters and goals of the investigation. Monteilh was "to gather information on Muslims in general," using information-gathering and surveillance tactics. The agents provided him with the tools to do so, including audio and video recording devices. They also gave Monteilh general goals, such as obtaining contact information from a certain number of Muslims per day, as well as specific tasks, such as entering a certain house or having lunch with a particular person. Sometimes, Allen and Armstrong prepared photo arrays with hundreds of Muslim community members and asked Monteilh to arrange the photos from most to least dangerous.

Armstrong and Allen did not, however, limit Monteilh to specific targets. Rather, "they repeatedly made clear

that they were interested simply in Muslims." Allen told Monteilh, "We want to get as many files on this community as possible." To the extent Allen and Armstrong expressed an interest in certain targets, it was in particularly religious Muslims and persons who might influence young Muslims. When Monteilh's surveillance activities generated information on non-Muslims, the agents set that information aside.

In accordance with his broad directive, Monteilh engaged with a wide variety of individuals. As instructed by his handlers, he attended classes at the mosque, amassed information on Muslims' charitable giving, attended Muslim fundraising events, collected information on community members' travel plans, attended lectures by Muslim scholars, went to daily prayers, memorized certain verses from the Quran and recited them to others, encouraged people to visit "jihadist" websites, worked out with targeted people at a gym to get close to them, and sought to obtain compromising information that could be used to pressure others to become informants. He also collected the names of board members, imams, teachers, and other leadership figures at the mosques, as well as the license plate numbers of cars in the mosque parking lots during certain events.

Virtually all of Monteilh's interactions with Muslims were recorded. Monteilh used audio and video recording devices provided to him by the agents, including a cellphone, two key fobs with audio recording capabilities, and a camera hidden in a button on his shirt. He recorded, for example, his interactions with Muslims in the mosques, which were transcribed and reviewed by FBI officials. He also recorded meetings and conversations in the mosque prayer hall to which he was not a

party. He did so by leaving his possessions behind, including his recording key fob, as though he had forgotten them or was setting them down while doing other things. Monteilh told Allen and Armstrong in written reports that he was recording conversations in this manner. The agents never told him to stop this practice, and they repeatedly discussed with Monteilh the contents of the recordings.

Armstrong and Allen occasionally instructed Monteilh to use his secret video camera for specific purposes, such as capturing the internal layout of mosques and homes. They also told Monteilh to obtain the contact information of people he met, and monitored his email and cellphone to obtain the email addresses and phone numbers of the people with whom he interacted.

Although Monteilh spent the majority of his time at ICOI, he conducted surveillance and made audio recordings in at least seven other mosques during the investigation. During Monteilh's fourteen months as an informant for Operation Flex, the FBI obtained from him hundreds of phone numbers; thousands of email addresses; background information on hundreds of individuals; hundreds of hours of video recordings of the interiors of mosques, homes, businesses, and associations; and thousands of hours of audio recordings of conversations, public discussion groups, classes, and lectures.

In addition to the surveillance undertaken directly by Monteilh, Allen and Armstrong told Monteilh that electronic surveillance equipment had been installed in at least eight mosques in the area, including ICOI. The electronic surveillance equipment installed at the Mission Viejo mosque was used to monitor Plaintiff Yassir Fazaga's conversations, including conversations held in

his office and other parts of the mosque not open to the public.

At the instruction of Allen and Armstrong, Monteilh took extensive handwritten notes each day about his activities and the surveillance he was undertaking. Allen and Armstrong met with Monteilh roughly twice each week to discuss his assignments, give him instructions, receive his daily notes, upload his recordings, and give him fresh devices. Monteilh was also required to call either Allen or Armstrong each day to apprise them of his activities. They told Monteilh that his daily notes were read by their supervisors.

The operation began to unravel when, in early 2007, Allen and Armstrong instructed Monteilh to begin more pointedly asking questions about jihad and armed conflict and to indicate his willingness to engage in violence. Implementing those instructions, Monteilh told several people that he believed it was his duty as a Muslim to take violent action and that he had access to weapons. Several ICOI members reported Monteilh to community leaders. One of the community leaders then called the FBI to report what Monteilh was saying, and instructed concerned ICOI members to call the Irvine Police Department, which they did. ICOI sought a restraining order against Monteilh, which was granted in June 2007.

Around the same time, Allen and Armstrong told Monteilh that Barbara Walls, then Assistant Special Agent in Charge of the FBI's Santa Ana office, no longer trusted him and wanted him to stop working for the FBI. In October 2007, Monteilh was told that his role in Operation Flex was over. At one of the final meetings between Monteilh and Agents Allen and Armstrong,

Walls was present. She warned Monteilh not to tell anyone about the operation.

Monteilh's identity as an informant was revealed in February 2009 in connection with a criminal prosecution for naturalization fraud of Ahmadullah (or Ahmed) Niazi, one of the ICOI members who had reported Monteilh's statements to the Irvine Police Department. FBI Special Agent Thomas Ropel testified at a bail hearing in Niazi's case that he had heard several recordings between Niazi and a confidential informant, and that the informant was the same person Niazi had reported to the police. Ropel's statements thus indicated that Monteilh was a confidential informant and that he had recorded numerous conversations for the FBI.

Several sources subsequently confirmed that Monteilh worked for the FBI, including the FBI and Monteilh himself. Although the FBI has disclosed some information about Monteilh's actions as an informant, including that he created audio and video recordings and provided handwritten notes to the FBI, the FBI maintains that "certain specific information" concerning Operation Flex and Monteilh's activities must be protected in the interest of national security.

II. Procedural History

Plaintiffs filed the operative complaint in September 2011, asserting eleven causes of action, which fall into two categories: claims alleging unconstitutional searches ("search claims") and claims alleging unlawful discrimination on the basis of, or burdens on, or abridgement of the rights to, religion ("religion claims"). The religion claims allege violations of the First Amendment Religion Clauses, the equal protection guarantee of the Due

Process Clause of the Fifth Amendment,[4] the Privacy Act, the Religious Freedom Restoration Act ("RFRA"), the Foreign Intelligence Surveillance Act ("FISA"), and the Federal Tort Claims Act ("FTCA").

Plaintiffs filed the complaint as a putative class action, with the class defined as "[a]ll individuals targeted by Defendants for surveillance or information-gathering through Monteilh and Operation Flex, on account of their religion, and about whom the FBI thereby gathered personally identifiable information." The complaint sought injunctive relief for the individual Plaintiffs and the class, and damages for themselves as individuals.[5] The Agent Defendants moved to dismiss the claims against them on various grounds, including qualified immunity. The Government moved to dismiss the amended complaint and for summary judgment, arguing that Plaintiffs' statutory and constitutional claims fail on various grounds unrelated to the state secrets privilege.

The Government also asserted that the religion claims, but not the search claims, should be dismissed under the *Reynolds* state secrets privilege, *see United States v. Reynolds*, 345 U.S. 1 (1953), on the ground that litigation of the religion claims could not proceed with-

---

[4] "The liberty protected by the Fifth Amendment's Due Process Clause contains within it the prohibition against denying to any person the equal protection of the laws." *United States v. Windsor*, 570 U.S. 744, 774 (2013) (citing *Bolling v. Sharpe*, 347 U.S. 497, 499-500 (1954)).

[5] The proposed class has not been certified. In addition to its relevance to the merits of Plaintiffs' claims, the information over which the Government asserted the state secrets privilege may also be relevant to the decision whether to certify the class. In addition, the scope of privileged evidence needed to litigate the case likely will differ should class certification be granted.

out risking the disclosure of certain evidence protected by the privilege. The assertion of the state secrets privilege was supported with a previously filed public declaration from then-U.S. Attorney General Eric Holder; a public declaration from Mark Giuliano, then Assistant Director of the FBI's Counterterrorism Division; and two classified declarations and a classified supplemental memorandum from Giuliano. The Attorney General asserted the state secrets privilege over three categories of evidence: (1) "[i]nformation that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation"; (2) "[i]nformation that could tend to reveal the initial reasons (*i.e.*, predicate) for an FBI counterterrorism investigation of a particular person (including in Operation Flex), any information obtained during the course of such an investigation, and the status and results of the investigation"; and (3) "[i]nformation that could tend to reveal whether particular sources and methods were used in a counterterrorism investigation."

In one order, the district court dismissed the FISA claim against the Government, brought under 50 U.S.C. § 1810, concluding that Congress did not waive sovereign immunity for damages actions under that statute. *See Al-Haramain Islamic Found., Inc. v. Obama* (*Al-Haramain II*), 705 F.3d 845, 850-55 (9th Cir. 2012). Plaintiffs do not challenge this dismissal. In the same order, the district court permitted Plaintiffs' FISA claim against the Agent Defendants to proceed, rejecting the argument that the Agent Defendants were entitled to qualified immunity.

In a second order, the district court dismissed all the other claims in the case on the basis of the *Reynolds*

state secrets privilege—including the Fourth Amendment claim, for which the Government Defendants expressly did not seek dismissal on that ground. Relying "heavily" on the classified declarations and supplemental memorandum, the district court concluded "that the subject matter of this action, Operation Flex, involves intelligence that, if disclosed, would significantly compromise national security." It held that the Government Defendants would need to rely on the privileged material to defend against Plaintiffs' claims, and that the privileged evidence was so inextricably tied up with nonprivileged material that "the risk of disclosure that further litigation would engender [could not] be averted through protective orders or restrictions on testimony." The district court declined to use, as a substitute for dismissal, the *in camera*, *ex parte* procedures set out in § 1806(f) of FISA, on the ground that FISA's procedures do not apply to non-FISA claims.

The Agent Defendants timely filed notices of appeal from the denial of qualified immunity on Plaintiffs' FISA claim. The district court then approved the parties' stipulation to stay all further proceedings related to the remaining FISA claim pending resolution of the Agent Defendants' appeal and, at Plaintiffs' request, entered partial final judgment under Federal Rule of Civil Procedure 54(b), allowing immediate appeal of the majority of Plaintiffs' claims. The Plaintiffs' appeal and the Agent Defendants' appeal from the denial of qualified immunity on the FISA claim were consolidated and are both addressed in this opinion.

DISCUSSION

We begin with the only claim to survive Defendants' motions to dismiss in the district court: the FISA claim

against the Agent Defendants. After addressing the FISA claim, we turn to Plaintiffs' argument that in cases concerning the lawfulness of electronic surveillance, the *ex parte* and *in camera* procedures set out in § 1806(f) of FISA supplant the dismissal remedy otherwise mandated by the state secrets evidentiary privilege. *See infra* Part II. We then proceed to evaluate Defendants' other arguments for dismissal of the search and religion claims. *See infra* Parts III-IV. Finally, we explain the procedures to be followed on remand. *See infra* Part V.

I. The FISA Claim Against the Agent Defendants

Section 110 of FISA, codified at 50 U.S.C. § 1810, creates a private right of action for an individual subjected to electronic surveillance in violation of FISA's procedures. It provides, in pertinent part:

> An aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation. . . .

50 U.S.C. § 1810.

This statutory text refers to another section, § 1809. That section, in turn, proscribes as criminal offenses two types of conduct: (1) "intentionally . . . engag[ing] in electronic surveillance under color of law except as authorized by [FISA, the Wiretap Act, the Stored Communications Act, or the pen register statute,] or any express statutory authorization," and (2) "intentionally . . . disclos[ing] or us[ing] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained

through electronic surveillance" without authorization. 50 U.S.C. § 1809(a).

To determine whether Plaintiffs plausibly allege a cause of action under § 1810, we must decide (1) whether Plaintiffs are "aggrieved persons" within the meaning of the statute, (2) whether the surveillance to which they were subjected qualifies as "electronic surveillance," and (3) whether the complaint plausibly alleges a violation of 50 U.S.C. § 1809.

An "aggrieved person" is defined as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k).[6] Plaintiffs allege in extensive detail in the complaint that they were subjected to many and varied instances of audio and video surveillance. The complaint's allegations are sufficient if proven to establish that Plaintiffs are "aggrieved persons."

The complaint also adequately alleges that much of the surveillance as described constitutes "electronic surveillance" as defined by FISA. FISA offers four definitions of electronic surveillance. 50 U.S.C. § 1801(f). Only the fourth is potentially at stake in this case:

> the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which *a person has a reasonable expectation of pri-*

---

[6] "'Person' means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power." 50 U.S.C. § 1801(m).

> *vacy* and *a warrant would be required for law enforcement purposes.*

Id. § 1801(f)(4) (emphases added). The key question as to the presence of "electronic surveillance" under this definition is whether the surveillance detailed in the complaint was undertaken in circumstances in which (1) Plaintiffs had a reasonable expectation of privacy and (2) a warrant would be required for law enforcement purposes. If, as the complaint alleges, no warrant was in fact obtained, such electronic surveillance would constitute a violation of § 1809. *Id.* § 1809(a).

The parties, citing *ACLU v. NSA*, 493 F.3d 644, 657 n.16, 683 (6th Cir. 2007), agree that these legal standards from FISA—reasonable expectation of privacy and the warrant requirement—are evaluated just as they would be under a Fourth Amendment analysis. The Agent Defendants argue, however, that they are entitled to qualified immunity on Plaintiffs' FISA claim. Plaintiffs accept that qualified immunity can apply under FISA but maintain that the Agent Defendants are not entitled to immunity.[7]

The Agent Defendants are entitled to qualified immunity from damages unless Plaintiffs "plead[] facts showing (1) that the official[s] violated a statutory or

---

[7] We have found only one decision, unpublished, addressing whether qualified immunity is an available defense to a FISA claim. *See Elnashar v. U.S. Dep't of Justice*, No. CIV.03-5110(JNE/JSM), 2004 WL 2237059, at *5 (D. Minn. Sept. 30, 2004) (dismissing a FISA claim on grounds of qualified immunity because there was no evidence the defendant "would have known that the search of [plaintiff's] apartment would have required a warrant"), *aff'd on other grounds*, 446 F.3d 792 (8th Cir. 2006). As the issue is not contested, we do not decide it.

constitutional right, and (2) that the right was 'clearly established' at the time of the challenged conduct." *Ashcroft v. al-Kidd*, 563 U.S. 731, 735 (2011) (quoting *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982)). We are permitted to "exercise [our] sound discretion in deciding which of the two prongs of the qualified immunity analysis should be addressed first in light of the circumstances in the particular case at hand." *Pearson v. Callahan*, 555 U.S. 223, 236 (2009). Because, as we conclude in *infra* Part II.E, the applicability of FISA's alternative procedures for reviewing state secrets evidence turns on whether the surveillance at issue constitutes "electronic surveillance" within the meaning of FISA,[8] we will begin with the first prong, even though we conclude that the Agent Defendants are ultimately entitled to qualified immunity on the second prong.

For purposes of qualified immunity, a right is clearly established if, "at the time of the challenged conduct, '[t]he contours of [a] right [are] sufficiently clear' that every 'reasonable official would have understood that what he is doing violates that right.'" *al-Kidd*, 563 U.S. at 741 (alterations in original) (quoting *Anderson v. Creighton*, 483 U.S. 635, 640 (1987)). "This inquiry . . . must be undertaken in light of the specific context of the case, not as a broad general proposition." *Saucier v. Katz*, 533 U.S. 194, 201 (2001). "We do not require a case directly on point, but existing precedent must have

---

[8] Again, as we noted above, "electronic surveillance" as defined by FISA must fall under one of four types of government action. 50 U.S.C. § 1801(f). The relevant one for our purposes involves "the installation or use of an electronic, mechanical, or other surveillance device . . . under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." *Id.* § 1801(f)(4).

placed the statutory or constitutional question beyond debate." *al-Kidd*, 563 U.S. at 741.

"The operation of [the qualified immunity] standard, however, depends substantially upon the level of generality at which the relevant 'legal rule' is to be identified." *Anderson*, 483 U.S. at 639. Often, whether a right is "clearly established" for purposes of qualified immunity will turn on the legal test for determining whether that right has been violated. For claims of excessive force, for example, "[i]t is sometimes difficult for an officer to determine how the relevant legal doctrine . . . will apply to the factual situation the officer confronts." *Saucier*, 533 U.S. at 205. "The calculus of reasonableness must embody allowance for the fact that police officers are often forced to make split-second judgments —in circumstances that are tense, uncertain, and rapidly evolving— about the amount of force that is necessary in a particular situation." *Graham v. Connor*, 490 U.S. 386, 396-97 (1989). By contrast, "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no," *Kyllo v. United States*, 533 U.S. 27, 31 (2001), as "the Fourth Amendment has drawn a firm line at the entrance to the house," *Payton v. New York*, 445 U.S. 573, 590 (1980). Thus, where the test for determining whether the right in question has been violated is framed as a standard, rather than a rule, officials are given more breathing room to make "reasonable mistakes." *Saucier*, 533 U.S. at 205. In those instances, we require a higher degree of factual specificity before concluding that the right is "clearly established." But where the right at issue is clear and specific, officials may not claim qualified im-

munity based on slight changes in the surrounding circumstances.[9]

To properly approach this inquiry, we consider separately three categories of audio and video surveillance alleged in the complaint: (1) recordings made by Monteilh of conversations to which he was a party; (2) recordings made by Monteilh of conversations to which he was not a party (i.e., the recordings of conversations in the mosque prayer hall); and (3) recordings made by devices planted by FBI agents in Fazaga's office and AbdelRahim's house, car, and phone.[10]

---

[9] The Supreme Court made a similar observation in an analogous context—determining whether a state court has unreasonably applied clearly established federal law for purposes of habeas review under the Antiterrorism and Effective Death Penalty Act: "[T]he range of reasonable judgment can depend in part on the nature of the relevant rule. If a legal rule is specific, the range may be narrow. . . . Other rules are more general, and their meaning must emerge in application over the course of time." *Yarborough v. Alvarado*, 541 U.S. 652, 664 (2004).

[10] We note that, in their "Claims for Relief," under the FISA cause of action, Plaintiffs recite that "Defendants, under color of law, *acting through Monteilh*" violated FISA (emphasis added). But the complaint specifically recites facts relating to devices allegedly planted directly by the Agent Defendants. Under the Federal Rules of Civil Procedure, it is the facts alleged that circumscribe the reach of the complaint for purposes of a motion to dismiss. *See Skinner v. Switzer*, 562 U.S. 521, 530 (2011).

We also note that there may be a fourth category of surveillance here at issue: video recordings of the interiors of individuals' homes. These recordings are not given meaningful attention in the parties' briefs, and we cannot determine from the complaint if Plaintiffs mean to allege that Monteilh video recorded the layouts of houses into which he was invited, or that he entered the houses without permission. Although at this stage we do not construe the complaint as asserting claims based on this fourth category of surveillance, our

We conclude that the Agent Defendants are entitled to dismissal on qualified immunity grounds of Plaintiffs' § 1810 claim as to the first two categories of surveillance. As to the third category of surveillance, conducted via devices planted in AbdelRahim's house and Fazaga's office, Allen and Armstrong are not entitled to qualified immunity. But Tidwell, Walls, and Rose are entitled to dismissal as to this category, because Plaintiffs do not plausibly allege their involvement in this category of surveillance, and so have not "pleaded facts showing . . . that [those] officials violated a statutory or constitutional right." *al-Kidd*, 563 U.S. at 735.

A. Recordings of Conversations to Which Monteilh Was a Party

A reasonable expectation of privacy exists where "a person ha[s] exhibited 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); *see, e.g.*, *California v. Ciraolo*, 476 U.S. 207, 211) (1986) (describing Justice Harlan's test as the "touchstone of Fourth Amendment analysis"). Generally, an individual "has no privacy interest in that which he voluntarily reveals to a government agent," a principle known as the invited informer doctrine. *United States v. Wahchumwah*, 710 F.3d 862, 867 (9th Cir. 2013) (citing *Hoffa v. United States*, 385 U.S. 293, 300-02 (1966)); *see also United States v. Aguilar*, 883 F.2d 662, 697-98 (9th Cir. 1989), *superseded on other grounds by statute*, Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359, *as recognized in United States v.*

---

opinion does not foreclose Plaintiffs from clarifying these and other allegations on remand.

Gonzalez-Torres, 309 F.3d 594 (9th Cir. 2002). Plaintiffs contend, however, that the invited informer doctrine does not apply to the recordings made by Monteilh of conversations to which he was a party because the surveillance was conducted with discriminatory purpose and therefore in bad faith.

Bad faith of this sort does not, however, implicate the reasonable privacy expectation protected by the Fourth Amendment or violate the Fourth Amendment's warrant requirement. There is, to be sure, an important "limitation[] on the government's use of undercover informers to infiltrate an organization engaging in protected first amendment activities": the government's investigation must not be conducted "for the purpose of abridging first amendment freedoms." *Aguilar*, 883 F.2d at 705. But that limitation on voluntary conversations with undercover informants—sometimes referred to as a "good faith" requirement,[11] *e.g.*, *United States v. Mayer*, 503 F.3d 740, 751 (9th Cir. 2007); *Aguilar*, 883 F.2d at 705—is imposed by the First Amendment, not the Fourth Amendment. As that constitutional limitation is not grounded in privacy expectations, it does not affect the warrant requirement under the Fourth Amendment.

Under the appropriate Fourth Amendment precepts, "[u]ndercover operations, in which the agent is a so-called 'invited informer,' *are not* '*searches*' under the Fourth Amendment." *Mayer*, 503 F.3d at 750 (emphasis added) (quoting *Aguilar*, 883 F.2d at 701). "[A] defendant generally has *no* privacy interest"—not merely an

[11] We use this term in the remainder of this discussion to refer to the constitutional limitation on the use of informants discussed in the text.

unreasonable privacy interest—"in that which he voluntarily reveals to a government agent." *Wahchumwah*, 710 F.3d at 867 (emphasis added). In other words, use of a government informant under the invited informer doctrine—even if not in good faith in the First Amendment sense—does not implicate the privacy interests protected by the Fourth Amendment. Because our inquiry under FISA is confined to whether a reasonable expectation of privacy was violated and whether a warrant was therefore required, *see ACLU*, 493 F.3d at 657 n.16, 683, the First Amendment-grounded good-faith limitation does not apply to our current inquiry.

Under the invited informer doctrine, Plaintiffs lacked a reasonable expectation of privacy in the conversations recorded by Monteilh to which he was a party. The Agent Defendants are therefore not liable under FISA for this category of surveillance.

B. Recordings of Conversations in the Mosque Prayer Hall to Which Monteilh Was Not a Party

Plaintiffs did have a privacy-grounded reasonable expectation that their conversations in the mosque prayer hall would not be covertly recorded by an individual who was not present where Plaintiffs were physically located and was not known to be listening in.[12] The Agent Defendants are, however, entitled to qualified immunity with respect to this category of surveillance under the second prong of the qualified immunity standard—whether "the right was 'clearly established' at the time

---

[12] We are not suggesting that the recording would have been impermissible under FISA and the Fourth Amendment if the Agent Defendants had obtained a warrant based on probable cause. Here, however, no warrant was obtained.

of the challenged conduct." *al-Kidd*, 563 U.S. at 735 (quoting *Harlow*, 457 U.S. at 818).

Again, the relevant questions here on the merits of the FISA and Fourth Amendment issues are whether "a person ha[s] exhibited an actual (subjective) expectation of privacy," and whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring). To first determine whether an individual has "exhibited an actual expectation of privacy," we assess whether "he [sought] to preserve [something] as private." *Bond v. United States*, 529 U.S. 334, 338 (2000) (alterations in original) (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). Based on the rules and customs of the mosque, and the allegations in the complaint, we have no trouble determining that Plaintiffs manifested an actual, subjective expectation of privacy in their conversations there.

The mosque prayer hall is not an ordinary public place. It is a site of religious worship, a place for Muslims to come together for prayer, learning, and fellowship. Plaintiffs allege that the prayer hall "is [a] sacred space where particular rules and expectations apply. Shoes are prohibited, one must be in a state of ablution, discussing worldly matters is discouraged, and the moral standards and codes of conduct are at their strongest." Notably, "[g]ossiping, eavesdropping, or talebearing (*namima*—revealing anything where disclosure is resented) is forbidden." And ICOI, which Malik and AbdelRahim attended, specifically prohibited audio and video recording in the mosque without permission. When, on a rare occasion, an outside entity did record an event or a speaker, ICOI put up signs to notify congregants. Furthermore, Plaintiffs explain in their com-

plaint that *halaqas*, which are small group meetings during which participants "discuss theology or matters related to the practice of Islam," are understood by mosque attendees to be environments that "ensure some measure of confidentiality among participants."[13]

These privacy-oriented rules and customs confirm for us that Plaintiffs held a subjective expectation of privacy in their conversations among themselves while in the prayer hall.

That Plaintiffs were not alone in the mosque prayer hall does not defeat their claim that they manifested an expectation of privacy.[14] "Privacy does not require solitude." *United States v. Taketa*, 923 F.2d 665, 673 (9th Cir. 1991). For example, "a person can have a subjective expectation that his or her home will not be searched by

---

[13] We understand that description to imply that Monteilh recorded conversations that occurred during *halaqas* in the mosque prayer hall.

[14] The Agent Defendants cite *Smith v. Maryland*, 442 U.S. at 740-41, to support the proposition that the unattended recordings in the mosque prayer hall did not invade Plaintiffs' reasonable expectation of privacy. *Smith* and its progeny do not apply here. *Smith* concerned a pen register installed and used by a telephone company, and held that an individual enjoys no Fourth Amendment protection "in information he voluntary turns over to third parties." *Id.* at 743-44. But, as the Fourth Circuit has stressed, *Smith* and the cases relying on it are concerned with "whether the government invades an individual's reasonable expectation of privacy when it obtains, *from a third party*, the third party's records." *United States v. Graham*, 824 F.3d 421, 426 (4th Cir. 2016) (en banc) (emphasis added), *abrogated on other grounds by Carpenter v. United States*, 138 S. Ct. 2206 (2018). Cases "involv[ing] *direct* government surveillance activity," including surreptitiously viewing, listening to, or recording individuals—like the one before us—present a wholly separate question. *Id.*

the authorities, even if he or she has invited friends into his or her home." *Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1102 (C.D. Cal. 2006), *aff'd sub nom. Bernhard v. City of Ontario*, 270 F. App'x 518 (9th Cir. 2008). The same principle applies to certain other enclosed locations in which individuals have particular reason to expect confidentiality and repose.[15]

Finally, the case law distinguishes between an expectation of privacy in a place and an expectation of privacy as to whether an individual's conversations or actions in that place would be covertly recorded by persons not themselves present in that place.[16] The Supreme Court has recently emphasized the significant difference between obtaining information in person and recording information electronically. *See Carpenter*, 138 S. Ct. at 2219 ("Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their

---

[15] *Taketa*, for example, held that a state employee could hold an expectation of privacy in his office even though the office was shared with two others. 923 F.2d at 673. "[E]ven 'private' business offices are often subject to the legitimate visits of coworkers, supervisors, and the public, without defeating the expectation of privacy unless the office is 'so open to fellow employees or the public that no expectation of privacy is reasonable.'" *Id.* (quoting *O'Connor v. Ortega*, 480 U.S. 709, 717-18 (1987)).

[16] *See also Taketa*, 923 F.2d at 676 ("Taketa has no general privacy interest in [his co-worker's] office, but he may have an expectation of privacy against being videotaped in it."); *Trujillo*, 428 F. Supp. 2d at 1102 (considering the secret installation and use of a video camera in a police department's men's locker room, and explaining that it was "immaterial" that the plaintiffs changed their clothes in the presence of others, because "[a] person can have a subjective expectation of privacy that he or she will not be *covertly recorded*, even though he or she knows there are other people in the locker room" (emphasis added)).

memory is nearly infallible."). Here, given the intimate and religious nature of the space and the express prohibition on recording, Plaintiffs have adequately alleged that they subjectively believed their conversations would not be covertly recorded by someone not present in the prayer hall for transmission to people not present in the prayer hall.[17]

Having concluded that Plaintiffs exhibited a subjective expectation of privacy, we now consider whether it was "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring). In assessing whether an individual's expectation of privacy is reasonable, context is key. *See O'Connor*, 480 U.S. at 715. "Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'" *Carpenter*, 138 S. Ct. at 2213-14 (alteration in original) (footnote omitted) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)). Relevant here is the principle that "the extent to which the Fourth Amendment protects people may depend upon *where* those people are." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (emphasis added). We thus "assess the nature of the location where [the] conversations were seized"—here, the mosque prayer hall. *United States v. Gonzalez, Inc.*, 412

[17] The complaint alleges that Plaintiffs lost "confidence in the mosque as a sanctuary" after learning of Monteilh's surveillance. This feeling of the *loss* of privacy reinforces the conclusion that Plaintiffs exhibited an actual expectation of privacy in their conversations in the mosque before the alleged surveillance took place.

F.3d 1102, 1116-17 (9th Cir. 2005), *amended on denial of reh'g*, 437 F.3d 854 (9th Cir. 2006).

The sacred and private nature of the houses of worship Plaintiffs attended distinguishes them from the types of commercial and public spaces in which courts have held that individuals lack a reasonable expectation of privacy.[18] *United States v. Gonzalez*, 328 F.3d 543 (9th Cir. 2003), for example, held that the defendant had no reasonable expectation of privacy in "a large, quasi-public mailroom at a public hospital during ordinary business hours." *Id.* at 547. The mailroom had open doors, was visible to the outside via large windows, and received heavy foot traffic. *Id.* In addition to focusing on the physical specifics of the mailroom, *Gonzalez* emphasized that public hospitals, "by their nature . . . create a diminished expectation of privacy. The use of surveillance cameras in hospitals for patient protection, for documentation of medical procedures and to prevent theft of prescription drugs is not uncommon." *Id.* The mosque prayer halls in this case, by contrast, have no characteristics similarly evidencing diminished expectations of privacy or rendering such expectations unreasonable.[19] There are no urgent health or safety needs

---

[18] *See, e.g., In re John Doe Trader No. One*, 894 F.2d 240, 243-44 (7th Cir. 1990) (holding that a rule prohibiting tape recorders on the trading floor "aimed at various forms of distracting behavior" and explicitly "designed to protect 'propriety and decorum' not privacy" did not support a reasonable expectation of privacy).

[19] Again, the fact that many people worshipped at the mosque does not render the Plaintiffs' expectations of privacy in their conversations (or at the very least from, their expectations that their conversations would not be covertly recorded) unreasonable. In *Gonzalez, Inc.*, for example, we held that individuals who owned and managed a small, family-run business with up to 25 employees had "a reason-

justifying surveillance. And the use of surveillance equipment at ICOI is not only uncommon, but expressly forbidden.

Our constitutional protection of religious observance supports finding a reasonable expectation of privacy in such a sacred space, where privacy concerns are acknowledged and protected, especially during worship and other religious observance. *Cf. Mockaitis v. Harcleroad*, 104 F.3d 1522, 1533 (9th Cir. 1997) (holding that, based in part on "the nation's history of respect for religion in general," a priest had a reasonable expectation of privacy in his conversation with an individual during confession), *overruled on other grounds by City of Boerne v. Flores*, 521 U.S. 507 (1997). Thus, Plaintiffs' expectation that their conversations in the mosque prayer hall would be confidential among participants (unless shared by one of them with others), and so would not be intercepted by recording devices planted by absent government agents was objectively reasonable.

Finally, "[w]here the materials sought to be seized may be protected by the First Amendment, the require-

---

able expectation of privacy over the on-site business conversations between their agents." 412 F.3d at 1116-17. The Gonzalez family, whose phone calls were intercepted, were not alone in their place of business, and their calls could have been overheard by others who were present. But we concluded that they nonetheless had a reasonable expectation of privacy over their conversations because they owned the office, had full access to the building, and exercised managerial control over the office's day-to-day operations. *Id.* Similarly, *United States v. McIntyre*, 582 F.2d 1221 (9th Cir. 1978), rejected the argument that a police officer lacked a reasonable expectation of privacy over conversations had in his office because his office door was open and a records clerk worked nearby in an adjacent room. *Id.* at 1224. "A business office need not be sealed to offer its occupant a reasonable degree of privacy," we reasoned. *Id.*

ments of the Fourth Amendment must be applied with 'scrupulous exactitude.'" *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). "National security cases," like the one here, "often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime." *United States v. U.S. District Court* (*Keith*), 407 U.S. 297, 313 (1972). "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy. . . . " *Id.* at 314.

Accordingly, we hold that Plaintiffs had a reasonable expectation of privacy that their conversations in the mosque prayer hall would not be covertly recorded by a government agent not party to the conversations.

As of 2006 and 2007, however, no federal or state court decision had held that individuals generally have a reasonable expectation of privacy from surveillance in places of worship. Our court had declined to read *Katz* as established authority "for the proposition that a reasonable expectation of privacy attaches to church worship services open to the public." *The Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518, 527 (9th Cir. 1989). Noting that there was a lack of clearly established law so concluding, *Presbyterian Church* held that Immigration and Naturalization Service ("INS") officials were entitled to qualified immunity from a Fourth Amendment challenge to undercover electronic surveillance of church services conducted without a warrant and without probable cause. *Id.* No case decided between *Presbyterian Church* and the incidents giving rise to this case decided otherwise. And no case decided during that period addressed circumstances more like

those here, in which there are some specific manifestations of an expectation of privacy in the particular place of worship. Arguably pertinent was *Mockaitis*, but that case concerned the confession booth, not the church premises generally. 104 F.3d at 1533. The circumstances here fall between *Presbyterian Church* and *Mockaitis*, so there was no clearly established law here applicable. The Agent Defendants are thus entitled to qualified immunity as to this category of surveillance.

C. Recordings Made by Planted Devices

It was, of course, clearly established in 2006 and 2007 that individuals have a reasonable expectation of privacy from covert recording of conversations in their homes, cars, and offices, and on their phones. *See, e.g.*, *Kyllo*, 533 U.S. at 31 (home); *New York v. Class*, 475 U.S. 106, 115 (1986) (cars); *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring) (enclosed telephone booths); *Taketa*, 923 F.2d at 673 (office); *McIntyre*, 582 F.2d at 1223-24 (office). The Agent Defendants accept these well-established legal propositions. But they maintain that the complaint's allegations that the FBI planted electronic surveillance equipment in Fazaga's office and AbdelRahim's house, car, and phone are too conclusory to satisfy *Iqbal*'s plausibility standard, and so do not adequately allege on the merits a violation of Plaintiffs' rights under FISA. *See al-Kidd*, 563 U.S. at 735; *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009). We cannot agree.

Plaintiffs offer sufficient well-pleaded facts to substantiate their allegation that some of the Agent Defendants—Allen and Armstrong—were responsible for planting devices in AbdelRahim's house. Specifically, the complaint details one occasion on which Allen

and Armstrong asked Monteilh about something that had happened in AbdelRahim's house that Monteilh had not yet communicated to them, and explained that they knew about it because they had audio surveillance in the house.

Plaintiffs also allege sufficient facts with regard to those two Agent Defendants in support of their allegation of electronic surveillance of Fazaga's office in the OCIF mosque in Mission Viejo: Allen and Armstrong told Monteilh that electronic surveillance was "spread indiscriminately" across "at least eight area mosques including ICOI, and mosques in Tustin, Mission Viejo, Culver City, Lomita, West Covina, and Upland," and that "they could get in a lot of trouble if people found out what surveillance they had in the mosques." They also instructed Monteilh to use a video camera hidden in a shirt button to record the interior of OCIF and "get a sense of the schematics of the place—entrances, exits, rooms, bathrooms, locked doors, storage rooms, as well as security measures and whether any security guards were armed." Armstrong later told Monteilh that he and Allen used the information he recorded to enter OCIF.

As to Tidwell, Walls, and Rose, however, the complaint does not plausibly allege their personal involvement with respect to the planted devices.[20] The complaint details Tidwell, Walls, and Rose's oversight of

---

[20] Because we concluded with respect to the first two categories of surveillance either that Plaintiffs had no reasonable expectation of privacy or that the expectation was not clearly established in the case law at the pertinent time, we reach the question whether Plaintiffs plausibly allege the personal involvement of Tidwell, Wall, and Rose only with respect to the third category of surveillance.

Monteilh, including that they read his daily notes and were apprised, through Allen and Armstrong, of the information he collected. But the complaint never alleges that *Monteilh* was involved in planting devices in AbdelRahim's house, car, or phone, or in Fazaga's office; those actions are attributed only to unnamed FBI agents.

The complaint also offers general statements that Tidwell, Walls, and Rose supervised Allen and Armstrong.[21] But "[g]overnment officials may not be held liable for the unconstitutional conduct of their subordinates under a theory of *respondeat superior*." *Iqbal*, 556 U.S. at 676. Instead, "a plaintiff must plead that each Government-official defendant, through the official's own individual actions, has violated the Constitution." *Id.* Plaintiffs have not done so as to this category of surveillance with regard to Tidwell, Walls, and Rose. The complaint does not allege that the supervisors knew of, much less ordered or arranged for, the planting of the recording devices in AbdelRahim's home or Fazaga's office, so the supervisors are entitled to qualified immunity as to that surveillance. *See, e.g.*, *Chavez v. United States*, 683 F.3d 1102, 1110 (9th Cir. 2012); *Ortez v. Washington County*, 88 F.3d 804, 809 (9th Cir. 1996).

In sum, Plaintiffs allege a FISA claim against Allen and Armstrong for recordings made by devices planted

---

[21] The relevant allegations were only that Walls and Rose "actively monitored, directed, and authorized the actions of Agents Allen and Armstrong and other agents at all times relevant in this action, for the purpose of surveilling Plaintiffs and other putative class members because they were Muslim" and that Tidwell "authorized and actively directed the actions of Agents Armstrong, Allen, Rose, Walls, and other agents."

by FBI agents in AbdelRahim's house and Fazaga's office. As to all other categories of surveillance, the Agent Defendants either did not violate FISA; are entitled to qualified immunity on the FISA claim because Plaintiffs' reasonable expectation of privacy was not clearly established; or were not plausibly alleged in the complaint to have committed any FISA violation that may have occurred.

II. The State Secrets Privilege and FISA Preemption

Having addressed the only claim to survive Defendants' motions to dismiss in the district court, we turn to the district court's dismissal of the remaining claims pursuant to the state secrets privilege.[22] Plaintiffs argue that reversal is warranted "on either of two narrower grounds." First, Plaintiffs argue that, at this preliminary stage, the district court erred in concluding that further litigation would require the disclosure of privileged information. Second, Plaintiffs maintain that the district court should have relied on FISA's alternative procedures for handling sensitive national security information. Because we agree with Plaintiffs' second argument, we do not decide the first. We therefore need not review the Government's state secrets claim to decide whether the standard for dismissal at this juncture —whether the district court properly "determine[d] with certainty . . . that litigation must be limited or cut off in order to protect state secrets, even before any discovery or evidentiary requests have been made," *Mohamed v.*

---

[22] Plaintiffs do not dispute at this juncture the district court's conclusion that the information over which the Attorney General asserted the state secrets privilege indeed comes within the privilege. We therefore assume as much for present purposes.

Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081 (9th Cir. 2010) (en banc)—has been met.

The initial question as to Plaintiffs' second argument is whether the procedures established under FISA for adjudicating the legality of challenged electronic surveillance replace the common law state secrets privilege with respect to such surveillance to the extent that privilege allows the categorical dismissal of causes of action. The question is a fairly novel one. We are the first federal court of appeals to address it. Only two district courts, both in our circuit, have considered the issue. Those courts both held that FISA "displace[s] federal common law rules such as the state secrets privilege with regard to matters within FISA's purview." *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1105-06 (N.D. Cal. 2013); *accord In re NSA Telecomms. Records Litig.* (*In re NSA*), 564 F. Supp. 2d 1109, 1117-24 (N.D. Cal. 2008). We rely on similar reasoning to that in those district court decisions, but reach a narrower holding as to the scope of FISA preemption.

Our analysis of this issue proceeds as follows. First, we offer a brief review of the state secrets privilege. Second, we discuss one reason why the district court should not have dismissed the search claims based on the privilege. Third, we explain why FISA displaces the dismissal remedy of the common law state secrets privilege as applied to electronic surveillance generally. Then we review the situations in which FISA's procedures under § 1806(f) apply, including affirmative constitutional challenges to electronic surveillance. Finally, we explain why the present case fits at least one of the situations in which FISA's procedures apply.

Before we go on, we emphasize that although we hold that Plaintiffs' electronic surveillance claims are not subject to outright dismissal at the pleading stage because FISA displaces the state secrets privilege, the FISA procedure is, not surprisingly, extremely protective of government secrecy. Under that procedure, Plaintiffs' religion claims will not go forward under the open and transparent processes to which litigants are normally entitled. Instead, in the interest of protecting national security, the stringent FISA procedures require severe curtailment of the usual protections afforded by the adversarial process and due process. *See, e.g.*, *Yamada v. Nobel Biocare Holding AG*, 825 F.3d 536, 545 (9th Cir. 2016) (holding that the district court's use of *ex parte*, *in camera* submissions to support its fee order violated defendants' due process rights); *Intel Corp. v. Terabyte Int'l, Inc.*, 6 F.3d 614, 623 (9th Cir. 1993) (same); *MGIC Indem. Corp. v. Weisman*, 803 F.2d 500, 505 (9th Cir. 1986) (same). As it is Plaintiffs who have invoked the FISA procedures, we proceed on the understanding that they are willing to accept those restrictions to the degree they are applicable as an alternative to dismissal, and so may not later seek to contest them.[23]

A. The State Secrets Privilege

"The Supreme Court has long recognized that in exceptional circumstances courts must act in the interest of the country's national security to prevent disclosure of state secrets, even to the point of dismissing a case entirely." *Jeppesen*, 614 F.3d at 1077 (citing *Totten v. United States*, 92 U.S. 105, 107 (1876)). Neither the Su-

[23] We discuss how the district court is to apply the FISA procedures to Plaintiffs' surviving claims on remand in *infra* Part V.

preme Court nor this court has precisely delineated what constitutes a state secret. *Reynolds* referred to "military matters which, in the interest of national security, should not be divulged." 345 U.S. at 10. *Jeppesen* added that not all classified information is necessarily privileged under *Reynolds*. 614 F.3d at 1082. The state secrets privilege has been held to apply to information that would result in "impairment of the nation's defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign governments, or where disclosure would be inimical to national security." *Black v. United States*, 62 F.3d 1115, 1118 (8th Cir. 1995) (citations and internal quotation marks omitted). But courts have acknowledged that terms like "military or state secrets" are "amorphous in nature," *id.* (citation omitted); the phrase "inimical to national security" certainly is. And although purely domestic investigations with no international connection do not involve state secrets, we recognize that the contours of the privilege are perhaps even more difficult to draw in a highly globalized, post-9/11 environment, where the lines between foreign and domestic security interests may be blurred.

We do not attempt to resolve the ambiguity or to explain definitively what constitutes a "state secret." But we note the ambiguity nonetheless at the outset, largely as a reminder that, as our court has previously noted, "[s]imply saying 'military secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege." *Al-Haramain Islamic Found., Inc. v. Bush* (*Al-Haramain I*), 507 F.3d 1190, 1203 (9th Cir. 2007).

Created by federal common law, the modern state secrets doctrine has two applications: the *Totten* bar and the *Reynolds* privilege. The *Totten* bar is invoked "'where the very subject matter of the action' is 'a matter of state secret.'" *Id.* at 1077 (quoting *Reynolds*, 345 U.S. at 11 n.26). It "completely bars adjudication of claims premised on state secrets." *Id.*; *see also Totten*, 95 U.S. at 106-07. The *Reynolds* privilege, by contrast, "is an evidentiary privilege rooted in federal common law." *Kasza v. Browner*, 133 F.3d 1159, 1167 (9th Cir. 1998); *see also Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 485 (2011). It "may be asserted at any time," and successful assertion "will remove the privileged evidence from the litigation." *Jeppesen*, 614 F.3d at 1079-80.

Here, after the Attorney General asserted the *Reynolds* privilege and the Government submitted both public and classified declarations setting out the parameters of its state secrets contention, the Government Defendants requested dismissal of Plaintiffs' religion claims in toto—but not the Fourth Amendment and FISA claims—at the pleading stage. "Dismissal at the pleading stage under *Reynolds* is a drastic result and should not be readily granted." *Jeppesen*, 614 F.3d at 1089. Only "if state secrets are so central to a proceeding that it cannot be litigated without threatening their disclosure" is dismissal the proper course. *Id.* at 1081 (quoting *El-Masri v. United States*, 479 F.3d 296, 308 (4th Cir. 2007)). Because there is a strong interest in allowing otherwise meritorious litigation to go forward, the court's inquiry into the need for the secret information should be specific and tailored, not vague and general. *See id.* at 1081-82; *In re Sealed Case*, 494 F.3d 139, 144-54 (D.C. Cir. 2007).

Specifically, the *Reynolds* privilege will justify dismissal of the action in three circumstances: (1) if "the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence"; (2) if "the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim"; and (3) if "privileged evidence" is "inseparable from nonprivileged information that will be necessary to the claims or defenses" such that "litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Jeppesen*, 614 F.3d at 1083 (citations omitted). The district court assumed that Plaintiffs could make a prima facie case without resorting to state secrets evidence, but determined that the second and third circumstances exist in this case and require dismissal.

B. The District Court's Dismissal of the Search Claims Based on the State Secrets Privilege

As a threshold matter, before determining whether FISA displaces the state secrets privilege with regard to electronic surveillance, we first consider which of Plaintiffs' claims might otherwise be subject to dismissal under the state secrets privilege. Although the Government expressly did not request dismissal of the Fourth Amendment and FISA claims based on the privilege, the district court nonetheless dismissed the Fourth Amendment claim on that basis. That was error.

The Government must formally claim the *Reynolds* privilege. *Reynolds*, 345 U.S. at 7-8. The privilege is "not simply an administrative formality" that may be asserted by any official. *Jeppesen*, 614 F.3d at 1080 (quoting *United States v. W.R. Grace*, 526 F.3d 499, 507-08 (9th Cir. 2008) (en banc)). Rather, the formal claim must

be "lodged by the head of the department which has control over the matter." *Reynolds*, 345 U.S. at 8. The claim must "reflect the certifying official's *personal* judgment; responsibility for [asserting the privilege] may not be delegated to lesser-ranked officials." *Jeppesen*, 614 F.3d at 1080. And the claim "must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Id.* Such unusually strict procedural requirements exist because "[t]he privilege 'is not to be lightly invoked,'" especially when dismissal of the entire action is sought. *Id.* (quoting *Reynolds*, 345 U.S. at 7).

Here, although the Government has claimed the *Reynolds* privilege over certain state secrets, it has not sought dismissal of the Fourth Amendment and FISA claims based on its invocation of the privilege. In light of that position, the district court should not have dismissed those claims. In doing so, its decision was inconsistent with *Jeppesen*'s observation that, "[i]n evaluating the need for secrecy, 'we acknowledge the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find ourselves second guessing the Executive in this arena.'" 614 F.3d at 1081-82 (quoting *Al-Haramain I*, 507 F.3d at 1203). Just as the Executive is owed deference when it asserts that exclusion of the evidence or dismissal of the case is necessary to protect national security, so the Executive is necessarily also owed deference when it asserts that national security is not threatened by litigation.

Indeed, *Jeppesen* cautioned that courts should work "to ensure that the state secrets privilege is asserted no

more frequently and sweepingly than necessary." *Id.* at 1082 (quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983)). Dismissing claims based on the privilege where the Government has expressly told the court it is not necessary to do so—and, in particular, invoking the privilege to dismiss, at the pleading stage, claims the Government has expressly told the court it need not dismiss on grounds of privilege—cuts directly against *Jeppesen*'s call for careful, limited application of the privilege.

Although the Government Defendants expressly did not request dismissal of the search claims under the state secrets privilege, the Agent Defendants did so request. In declining to seek dismissal of the search claims based on the state secrets privilege, the Government explained:

> At least at this stage of the proceedings, sufficient non-privileged evidence may be available to litigate these claims should they otherwise survive motions to dismiss on nonprivilege grounds. The FBI has previously disclosed in a separate criminal proceeding that Monteilh collected audio and video information for the FBI, and some of that audio and video information was produced in that prior case. The FBI has been reviewing additional audio and video collected by Monteilh for possible disclosure in connection with further proceedings on the issue of whether the FBI instructed or permitted Monteilh to leave recording devices unattended in order to collect non-consenting communications. The FBI expects that the majority of the audio and video will be available in connection with further proceedings. Thus, while it remains possible that the need to protect

> properly privileged national security information might still foreclose litigation of these claims, at present the FBI and official capacity defendants do not seek to dismiss these claims based on the privilege assertion.

The Agent Defendants note that the Government focuses on the public disclosure of recordings collected by Monteilh, and point out that Plaintiffs also challenge surveillance conducted without Monteilh's involvement —namely, the planting of recording devices by FBI agents in Fazaga's office and AbdelRahim's home, car, and phone. Allegations concerning the planting of recording devices by FBI agents other than Monteilh, the Agent Defendants argue, are the "sources and methods" discussed in the Attorney General's invocation of the privilege. The Agent Defendants thus maintain that because the Government's reasons for not asserting the privilege over the search claims do not apply to all of the surveillance encompassed by the search claims, dismissal as to the search claims is in fact necessary.

The Agent Defendants, however, are not uniquely subject to liability for the planted devices. The Fourth Amendment claim against the Government Defendants likewise applies to that category of surveillance. *See infra* Part III.A. The Agent Defendants—officials sued in their individual capacities—are not the protectors of the state secrets evidence; the Government is. Accordingly, and because the Agent Defendants have not identified a reason they specifically require dismissal to protect against the harmful disclosure of state secrets where the Government does not, we decline to accept their argu-

ment that the Government's dismissal defense must be expanded beyond the religion claims.[24]

In short, in determining *sua sponte* that particular claims warrant dismissal under the state secrets privilege, the district court erred. For these reasons, we will not extend FISA's procedures to challenges to the lawfulness of electronic surveillance to the degree the Government agrees that such challenges may be litigated in accordance with ordinary adversarial procedures without compromising national security.

C. FISA Displacement of the State Secrets Privilege

Before the enactment of FISA in 1978, foreign intelligence surveillance and the treatment of evidence implicating state secrets were governed purely by federal common law. Federal courts develop common law "in the absence of an applicable Act of Congress." *City of Milwaukee v. Illinois*, 451 U.S. 304, 313 (1981). "Federal common law is," however, "a 'necessary expedient' and when Congress addresses a question previously governed by a decision rested on federal common law the need for such an unusual exercise of lawmaking by federal courts disappears." *Id.* (citation omitted). Once "the field has been made the subject of comprehensive legislation or authorized administrative standards," fed-

---

[24] Although the Government may assert the state secrets privilege even when it is not a party to the case, *see Jeppesen*, 614 F.3d at 1080, we have not found—and the Agent Defendants have not cited—any case other than the one at hand in which a court granted dismissal under the privilege as to non-Government defendants, notwithstanding the Government's assertion that the claims at issue may be litigated with nonprivileged information.

eral common law no longer applies. *Id.* (quoting *Texas v. Pankey*, 441 F.2d 236, 241 (10th Cir. 1971)).

To displace federal common law, Congress need not "affirmatively proscribe[] the use of federal common law." *Id.* at 315. Rather, "to abrogate a common-law principle, the statute must 'speak directly' to the question addressed by the common law." *United States v. Texas*, 507 U.S. 529, 534 (1993) (quoting *Mobil Oil Corp. v. Higginbotham*, 436 U.S. 618, 625 (1978)). As we now explain, in enacting FISA, Congress displaced the common law dismissal remedy created by the *Reynolds* state secrets privilege as applied to electronic surveillance within FISA's purview.[25]

We have specifically held that because "the state secrets privilege is an evidentiary privilege rooted in federal common law . . . the relevant inquiry in deciding if [a statute] preempts the state secrets privilege is whether the statute '[speaks] *directly* to [the] question otherwise answered by federal common law.'" *Kasza*, 133 F.3d at 1167 (second and third alterations in original) (quoting *County of Oneida v. Oneida Indian Nation*, 470 U.S. 226, 236-37 (1985)).[26] Nonetheless, the Government maintains, in a vague and short paragraph in its brief, that Congress cannot displace the state secrets evidentiary privilege absent a clear statement, and that, because Plaintiffs cannot point to a clear state-

---

[25] Our holding concerns only the *Reynolds* privilege, not the *Totten* justiciability bar.

[26] Applying this principle, *Kasza* concluded that section 6001 of the Resource Conservation and Recovery Act ("RCRA"), 42 U.S.C. § 6961, did not preempt the state secrets privilege as to RCRA regulatory material, as "the state secrets privilege and § 6001 have different purposes." 133 F.3d at 1168.

ment, "principles of constitutional avoidance" require rejecting the conclusion that FISA's procedures displace the dismissal remedy of the state secrets privilege with regard to electronic surveillance.

In support of this proposition, the Government cites two out-of-circuit cases, *El-Masri v. United States*, 479 F.3d 296, and *Armstrong v. Bush*, 924 F.2d 282 (D.C. Cir. 1991). *El-Masri* does not specify a clear statement rule; it speaks generally about the constitutional significance of the state secrets privilege, while recognizing its common law roots. 479 F.3d at 303-04. *Armstrong* holds generally that the clear statement rule must be applied "to statutes that significantly alter the balance between Congress and the President," but does not apply that principle to the state secrets privilege. 924 F.2d at 289. So neither case is directly on point.

Under our circuit's case law, a clear statement in the sense of an explicit abrogation of the common law state secrets privilege is not required to decide that a statute displaces the privilege. Rather, if "the statute '[speaks] *directly* to [the] question otherwise answered by federal common law,'" that is sufficient. *Kasza*, 133 F.3d at 1167 (second and third alterations in original) (quoting *Oneida*, 470 U.S. at 236-37); *see also Texas*, 507 U.S. at 534. Although we, as a three-judge panel, could not hold otherwise, we would be inclined in any event to reject any clear statement rule more stringent than *Kasza*'s "speak directly to the question" requirement in this context.

The state secrets privilege may have "a constitutional 'core' or constitutional 'overtones,'" *In re NSA*, 564 F. Supp. 2d at 1124, but, at bottom, it is an evidentiary rule rooted in common law, *not* constitutional law. The

Supreme Court has so emphasized, explaining that *Reynolds* "decided a purely evidentiary dispute by applying evidentiary rules." *Gen. Dynamics*, 563 U.S. at 485. To require express abrogation, by name, of the state secrets privilege would be inconsistent with the evidentiary roots of the privilege.

In any event, the text of FISA does speak quite directly to the question otherwise answered by the dismissal remedy sometimes required by the common law state secrets privilege. Titled "In camera and ex parte review by district court," § 1806(f) provides:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, *the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was*

> *lawfully authorized and conducted*. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

50 U.S.C. § 1806(f) (emphasis added).

The phrase "notwithstanding any other law," the several uses of the word "whenever," and the command that courts "*shall*" use the § 1806(f) procedures to decide the lawfulness of the surveillance if the Attorney General asserts that national security is at risk, confirm Congress's intent to make the *in camera* and *ex parte* procedure the exclusive procedure for evaluating evidence that threatens national security in the context of electronic surveillance-related determinations. *Id.* (emphasis added). That mandatory procedure necessarily overrides, on the one hand, the usual procedural rules precluding such severe compromises of the adversary process and, on the other, the state secrets evidentiary dismissal option. *See* H.R. Rep. No. 95-1283, pt. 1, at 91 (1978) ("It is to be emphasized that, although a number of different procedures might be used to attack the legality of the surveillance, it is the procedures set out in subsections (f) and (g) 'notwithstanding any other law' that must be used to resolve the question.").[27]

---

[27] Whether "notwithstanding" language in a given statute should be understood to supersede all otherwise applicable laws or read more narrowly to override only previously existing laws depends on the overall context of the statute. *See United States v. Novak*, 476 F.3d 1041, 1046-47 (9th Cir. 2007) (en banc). Here, the distinction

The procedures set out in § 1806(f) are animated by the same concerns—threats to national security—that underlie the state secrets privilege. *See Jeppesen*, 614 F.3d at 1077, 1080. And they are triggered by a process—the filing of an affidavit under oath by the Attorney General—nearly identical to the process that triggers application of the state secrets privilege, a formal assertion by the head of the relevant department. *See id.* at 1080. In this sense, § 1806(f) "is, in effect, a 'codification of the state secrets privilege for purposes of relevant cases under FISA, as modified to reflect Congress's precise directive to the federal courts for the handling of [electronic surveillance] materials and information with purported national security implications.'" *Jewel*, 965 F. Supp. 2d at 1106 (quoting *In re NSA*, 564 F. Supp. 2d at 1119); *see also In re NSA*, 564 F. Supp. 2d at 1119 (holding that "the *Reynolds* protocol has no role where section 1806(f) applies"). That § 1806(f) requires *in camera* and *ex parte* review in the exact circumstance that could otherwise trigger dismissal of the case demonstrates that § 1806(f) supplies an alternative mechanism for the consideration of electronic state secrets evidence. Section 1806(f) therefore eliminates the need to dismiss the case entirely because of the absence of any legally sanctioned mechanism for a major modification of ordinary judicial procedures—*in camera*, *ex parte* decisionmaking.

This conclusion is consistent with the overall structure of FISA. FISA does not concern Congress and the President alone. Instead, the statute creates "a comprehensive, detailed program to regulate foreign intelli-

---

does not matter, as the *Reynolds* common law state secrets evidentiary privilege preceded the enactment of FISA.

gence surveillance in the domestic context." *In re NSA*, 564 F. Supp. 2d at 1118. FISA "set[s] out in detail roles for all three branches of government, providing judicial and congressional oversight of the covert surveillance activities by the executive branch combined with measures to safeguard secrecy necessary to protect national security." *Id.* at 1115. And it provides rules for the executive branch to follow in "undertak[ing] electronic surveillance and physical searches for foreign intelligence purposes in the domestic sphere." *Id.*

Moreover, FISA establishes a special court to hear applications for and grant orders approving electronic surveillance under certain circumstances. *See* 50 U.S.C. § 1803. FISA also includes a private civil enforcement mechanism, *see id.* § 1810, and sets out a procedure by which courts should consider evidence that could harm the country's national security, *see id.* § 1806(f). The statute thus broadly involves the courts in the regulation of electronic surveillance relating to national security, while devising extraordinary, partially secret judicial procedures for carrying out that involvement. And Congress expressly declared that FISA, along with the domestic law enforcement electronic surveillance provisions of the Wiretap Act and the Stored Communications Act, are "the exclusive means by which electronic surveillance . . . may be conducted." 18 U.S.C. § 2511(2)(f).

The legislative history of FISA confirms Congress's intent to displace the remedy of dismissal for the common law state secrets privilege. FISA was enacted in response to "revelations that warrantless electronic surveillance in the name of national security ha[d] been seriously abused." S. Rep. No. 95-604, pt. 1, at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908. The Senate

Select Committee to Study Governmental Operations with Respect to Intelligence Activities, a congressional task force formed in 1975 and known as the Church Committee, exposed the unlawful surveillance in a series of investigative reports. The Church Committee documented "a massive record of intelligence abuses over the years," in which "the Government ha[d] collected, and then used improperly, huge amounts of information about the private lives, political beliefs and associations of numerous Americans." S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, at 290 (1976). The Committee concluded that these abuses had "undermined the constitutional rights of citizens . . . primarily because checks and balances designed by the framers of the Constitution to assure accountability [were not] applied." *Id.* at 289.

Urging "fundamental reform," *id.* at 289, the Committee recommended legislation to "make clear to the Executive branch that it will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution," *id.* at 297. Observing that the Executive would have "no such authority after Congress has . . . covered the field by enactment of a comprehensive legislative charter" that would "provide the exclusive legal authority for domestic security activities," *id.* at 297, the Committee recommended that Congress create civil remedies for unlawful surveillance, both to "afford effective redress to people who are injured by improper federal intelligence activity" and to "deter improper intelligence activity," *id.* at 336. Further, in recognition of the potential interplay between promoting accountability and ensuring security, the Committee

noted its "belie[f] that the courts will be able to fashion discovery procedures, including inspection of material in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest." *Id.* at 337.

FISA implemented many of the Church Committee's recommendations. In striking a careful balance between assuring the national security and protecting against electronic surveillance abuse, Congress carefully considered the role previously played by courts, and concluded that the judiciary had been unable effectively to achieve an appropriate balance through federal common law:

> [T]he development of the law regulating electronic surveillance for national security purposes has been uneven and inconclusive. This is to be expected where the development is left to the judicial branch in an area where cases do not regularly come before it. Moreover, the development of standards and restrictions by the judiciary with respect to electronic surveillance for foreign intelligence purposes accomplished through case law threatens both civil liberties and the national security because that development occurs generally in ignorance of the facts, circumstances, and techniques of foreign intelligence electronic surveillance not present in the particular case before the court. . . . [T]he tiny window to this area which a particular case affords provides inadequate light by which judges may be relied upon to develop

> case law which adequately balances the rights of privacy and national security.

H. Rep. No. 95-1283, pt. 1, at 21. FISA thus represents an effort to "provide effective, reasonable safeguards to ensure accountability and prevent improper surveillance," and to "strik[e] a fair and just balance between protection of national security and protection of personal liberties." S. Rep. No. 95-604, pt. 1, at 7.

In short, the procedures outlined in § 1806(f) "provide[] a detailed regime to determine whether surveillance 'was lawfully authorized and conducted,'" *Al-Haramain I*, 507 F.3d at 1205 (citing 50 U.S.C. § 1806(f)), and constitute "Congress's specific and detailed description for how courts should handle claims by the government that the disclosure of material relating to or derived from electronic surveillance would harm national security," *Jewel*, 965 F. Supp. 2d at 1106 (quoting *In re NSA*, 564 F. Supp. 2d at 1119). Critically, the FISA approach does not publicly expose the state secrets. It does severely compromise Plaintiffs' procedural rights, but not to the degree of entirely extinguishing potentially meritorious substantive rights.

D. Applicability of FISA's § 1806(f) Procedures to Affirmative Legal Challenges to Electronic Surveillance

Having determined that, where they apply, § 1806(f)'s procedures displace a dismissal remedy for the *Reynolds* state secrets privilege, we now consider whether § 1806(f)'s procedures apply to the circumstances of this case.

By the statute's terms, the procedures set forth in § 1806(f) are to be used—where the Attorney General

files the requisite affidavit—in the following circumstances:

> [w]henever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter.

50 U.S.C. § 1806(f). From this text and the cross-referenced subsections, we derive three circumstances in which the *in camera* and *ex parte* procedures are to be used: when (1) a governmental body gives notice of its intent "to enter into evidence or otherwise use or disclose in *any* trial, hearing, or other proceeding in or before *any* court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance," *id.* § 1806(c) (emphases added);[28] (2) an aggrieved person moves to suppress the evidence, *id.* § 1806(e); or (3) an aggrieved person makes

---

[28] The text of § 1806(f) refers to notice "pursuant to subsection (c) *or* (d) of this section." 50 U.S.C. § 1806(f) (emphasis added). Section 1806(d) describes verbatim the same procedures as contained in § 1806(c), except as applied to States and political subdivisions rather than to the United States. *Id.* § 1806(d). For convenience, we refer only to § 1806(c) in this opinion, but our analysis applies to § 1806(d) with equal force.

"any motion or request . . . pursuant to *any* other statute or rule . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter," *id.* § 1806(f) (emphasis added).

The case at hand fits within the contemplated circumstances in two respects. First, although the Government has declined to confirm or deny in its public submissions that the information with respect to which it has invoked the state secrets privilege was obtained or derived from FISA-covered electronic surveillance of Plaintiffs, *see id.* § 1806(c), the complaint alleges that it was. The Attorney General's privilege assertion encompassed, among other things, "any information obtained during the course of" Operation Flex, the "results of the investigation," and "any results derived from" the "sources and methods" used in Operation Flex. It is precisely because the Government would like to use this information to defend itself that it has asserted the state secrets privilege. The district court's dismissal ruling was premised in part on the potential use of state secrets material to defend the case. Because the district court made the ruling after reviewing the surveillance materials, it is aware whether the allegations in the complaint concerning electronic surveillance are factually supported. Of course, if they are not, then the district court can decide on remand that the FISA procedures are inapplicable. For purposes of this opinion, we proceed on the premise that the Attorney General's invocation of the state secrets privilege relied on the potential use of material obtained or derived from electronic surveillance, as alleged in the complaint.

Second, in their prayer for relief, Plaintiffs have requested injunctive relief "ordering Defendants to destroy or return any information gathered through the unlawful surveillance program by Monteilh and/or Operation Flex described above, and any information derived from that unlawfully obtained information." Plaintiffs thus have requested, in the alternative, to "obtain" information gathered during or derived from electronic surveillance. *See id.* § 1806(f).

The Government disputes that FISA applies to this case. Its broader contention is that § 1806(f)'s procedures do not apply to any affirmative claims challenging the legality of electronic surveillance or the use of information derived from electronic surveillance, whether brought under FISA's private right of action or any other constitutional provision, statute, or rule. Instead, the Government maintains, FISA's procedures apply only when the government initiates the legal action, while the state secrets privilege applies when the government defends affirmative litigation brought by private parties.

The plain text and statutory structure of FISA provide otherwise. To begin, the language of the statute simply does not contain the limitations the Government suggests. As discussed above, § 1806(f)'s procedures are to be used in any one of three situations, each of which is separated in the statute by an "or." *See id.* The first situation—when "the Government intends to enter into evidence or otherwise use or disclose information obtained or derived from an electronic surveillance . . . against an aggrieved person" in "*any* trial, hearing, or other proceeding," *id.* § 1806(c) (emphasis added) —unambiguously encompasses affirmative as well as defen-

sive challenges to the lawfulness of surveillance.[29] The conduct governed by the statutory provision is the Government's intended entry into evidence or other use or disclosure of information obtained or derived from electronic surveillance. "[A]gainst an aggrieved person" refers to and modifies the phrase "any information obtained or derived." *Id.* As a matter of ordinary usage, the phrase "against an aggrieved person" cannot modify "any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States." *Id.* Evidence—such as "any information obtained or derived from an electronic surveillance"—can properly be said to be "against" a party. *See, e.g.*, U.S. Const. amend. V ("No person . . . shall be compelled in any criminal case to be *a witness against himself.* . . . "); *Miranda v. Arizona*, 384 U.S. 436, 460 (1966) ("[O]ur accusatory system of criminal justice demands that the government seeking

---

[29] In full, § 1806(c) reads:

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, 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, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

50 U.S.C. § 1806(c). Again, we refer to the text of § 1806(c) because § 1806(f)'s procedures apply "[w]henever a court or other authority is notified pursuant to subsection (c) or (d) of this section." *Id.* § 1806(f).

to punish an individual produce *the evidence against him* by its own independent labors, rather than by the cruel, simple expedient of compelling it from his own mouth." (emphasis added)). But a "trial, hearing, or other proceeding" is not for or against either party; such a proceeding is just an opportunity to introduce evidence. Also, as the phrase is set off by commas, "against an aggrieved person" is grammatically a separate modifier from the list of proceedings contained in § 1806(f). Were the phrase meant to modify the various proceedings, there would be no intervening comma setting it apart.

The third situation—when a "motion or request is made by an aggrieved person pursuant to any other statute or rule . . . before any court . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter," *id.* § 1806(f) —also by its plain text encompasses affirmative challenges to the legality of electronic surveillance. When an aggrieved person makes such a motion or request, or the government notifies the aggrieved person and the court that it intends to use or disclose information obtained or derived from electronic surveillance, the statute requires a court to use § 1806(f)'s procedures "to determine whether the surveillance . . . was lawfully authorized and conducted." *Id.* In other words, a court must "determine whether the surveillance was authorized and conducted in a manner which did not violate any constitutional or statutory right." S. Rep. No. 95-604, pt. 1, at 57; *accord* S. Rep. No. 95-701, at 63.

The inference drawn from the text of § 1806 is bolstered by § 1810, which specifically creates a private right of action for an individual subjected to electronic surveillance in violation of FISA. FISA prohibits, for example, electronic surveillance of a U.S. person "solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(2)(A). Here, Plaintiffs allege they were surveilled solely on account of their religion. If true, such surveillance was necessarily unauthorized by FISA, and § 1810 subjects any persons who intentionally engaged in such surveillance to civil liability. It would make no sense for Congress to pass a comprehensive law concerning foreign intelligence surveillance, expressly enable aggrieved persons to sue for damages when that surveillance is unauthorized, *see id.* § 1810, and provide procedures deemed adequate for the review of national security-related evidence, *see id.* § 1806(f), but not intend for those very procedures to be used when an aggrieved person sues for damages under FISA's civil enforcement mechanism. Permitting a § 1810 claim to be dismissed on the basis of the state secrets privilege because the § 1806(f) procedures are unavailable would dramatically undercut the utility of § 1810 in deterring FISA violations. Such a dismissal also would undermine the overarching goal of FISA more broadly—"curb[ing] the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604, pt. 1, at 8.

FISA's legislative history confirms that § 1806(f)'s procedures were designed to apply in both civil and criminal cases, and to both affirmative and defensive use of electronic surveillance evidence. The Senate bill ini-

tially provided a single procedure for criminal and civil cases, while the House bill at the outset specified two separate procedures for determining the legality of electronic surveillance.[30] In the end, the conference committee adopted a slightly modified version of the Senate bill, agreeing "that an *in camera* and *ex parte* proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases." H.R. Rep. No. 95-1720, at 32.

In the alternative, the Government suggests that § 1806(f)'s procedures for the use of electronic surveillance in litigation are limited to affirmative actions brought directly under § 1810. We disagree. The § 1806(f) procedures are expressly available, as well as mandatory, for affirmative claims brought "by an aggrieved person pursuant *to any . . . statute or rule* of the United States . . . before any court . . . of the United States." 50 U.S.C. § 1806(f) (emphasis added). This provision was meant "to make very clear that these procedures apply *whatever* the underlying rule or statute" at issue, so as "to prevent these carefully drawn procedures from being bypassed by the inventive litigant us-

---

[30] Under the House bill, in criminal cases there would be an *in camera* proceeding, and the court could, but need not, disclose the materials relating to the surveillance to the aggrieved person "if there were a reasonable question as to the legality of the suveillance [sic] and if disclosure would likely promote a more accurate determination of such legality, or if disclosure would not harm the national security." H.R. Rep. No. 95-1720, at 31 (1978) (Conf. Rep.), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060. In civil suits, there would be an *in camera* and *ex parte* proceeding before a court of appeals, and the court would disclose to the aggrieved person the materials relating to the surveillance "only if necessary to afford due process to the aggrieved person." *Id.* at 32.

ing a new statute, rule or judicial construction." H.R. Rep. No. 95-1283, pt. 1, at 91 (emphasis added).

Had Congress wanted to limit the use of § 1806(f)'s procedures only to affirmative claims alleging lack of compliance with FISA itself, it could have so specified, as it did in § 1809 and § 1810. Section 1810 creates a private right of action only for violations of § 1809. 50 U.S.C. § 1810. Section 1809 prohibits surveillance not authorized by FISA, the Wiretap Act, the Stored Communications Act, and the pen register statute. *Id.* § 1809(a). That § 1809 includes only certain, cross-referenced statutes while § 1810 is limited to violations of § 1809 contrasts with the broad language of § 1806(f) as to the types of litigation covered—litigation "pursuant *to any . . . statute or rule* of the United States." *Id.* § 1806(f) (emphasis added).

Furthermore, if—as here—an aggrieved person brings a claim under § 1810 and a claim under another statute or the Constitution based on the same electronic surveillance as is involved in the § 1810 claim, it would make little sense for § 1806(f) to require the court to consider *in camera* and *ex parte* the evidence relating to electronic surveillance for purposes of the claim under § 1810 of FISA but not permit the court to consider the exact same evidence in the exact same way for purposes of the non-FISA claim. Once the information has been considered by a federal judge *in camera* and *ex parte*, any risk of disclosure—which Congress necessarily considered exceedingly small or it would not have permitted such examination—has already been incurred. There would be no point in dismissing other claims because of that same concern.

We are not the first to hold that § 1806(f)'s procedures may be used to adjudicate claims beyond those arising under § 1810. The D.C. Circuit expressly so held in *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457 (D.C. Cir. 1991):

> When a district court conducts a § 1806(f) review, its task is not simply to decide whether the surveillance complied with FISA. Section 1806(f) requires the court to decide whether the surveillance was "lawfully authorized and conducted." The Constitution is law. Once the Attorney General invokes § 1806(f), the respondents named in that proceeding therefore must present not only their statutory but also their constitutional claims for decision.

Id. at 465; *accord United States v. Johnson*, 952 F.2d 565, 571-73, 571 n.4 (1st Cir. 1991) (using § 1806(f)'s *in camera* and *ex parte* procedures to review constitutional challenges to FISA surveillance).

In sum, the plain language, statutory structure, and legislative history demonstrate that Congress intended FISA to displace the state secrets privilege and its dismissal remedy with respect to electronic surveillance. Contrary to the Government's contention, FISA's § 1806(f) procedures are to be used when an aggrieved person affirmatively challenges, in any civil case, the legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law.[31]

---

[31] The Agent Defendants suggest that using the § 1806 procedures would violate their Seventh Amendment jury trial right and their due process rights.

E. Aggrieved Persons

We now consider more specifically whether FISA's § 1806(f) procedures may be used in this case. Because

---

Any Seventh Amendment argument is premature. Any hypothetical interference with a jury trial would arise only if a series of contingencies occurred on remand. First, given our various rulings precluding certain of Plaintiffs' claims and the narrow availability of *Bivens* remedies under current law, there are likely to be few, if any, remaining *Bivens* claims against the Agent Defendants. See *infra* Part I; *supra* Part III.B; *supra* Part IV.B. Second, as to any remaining claims against the Agent Defendants, the district court might determine that there was no unlawful surveillance after reviewing the evidence under the *in camera*, *ex parte* procedures, or the Agent Defendants may prevail on summary judgment. Moreover, it is possible that the district court's determination of whether the surveillance was lawful will be a strictly legal decision—analogous to summary judgment—made on the record supplied by the government. *See Parklane Hosiery Co. v. Shore*, 439 U.S. 322, 336 (1979) (noting that procedural devices like summary judgment are not "inconsistent" with the Seventh Amendment).

Should the various contingencies occur and leave liability issues to be determined, the Agent Defendants are free at that time to raise their Seventh Amendment arguments on remand. But, as the Seventh Amendment issue was not decided by the district court, may never arise, and, if it does, may depend on the merits on exactly how it arises, we decline to address the hypothetical constitutional question now.

With respect to the Agent Defendants' due process arguments, we and other courts have upheld the constitutionality of FISA's *in camera* and *ex parte* procedures with regard to criminal defendants. *See United States v. Abu-Jihaad*, 630 F.3d 102, 117-29 (2d Cir. 2010); *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Ott*, 827 F.2d 473, 476-77, 477 n.5 (9th Cir. 1987); *United States v. Belfield*, 692 F.2d 141, 148-49 (D.C. Cir. 1982); *United States v. Nicholson*, 955 F. Supp. 588, 590-92, 590 n.3 (E.D. Va. 1997) (collecting cases). Individual defendants in a civil suit are not entitled to more stringent protections than criminal defendants.

the procedures apply when evidence will be introduced "against an aggrieved person," 50 U.S.C. § 1806(c), and when "any motion or request is made by an aggrieved person," *id.* § 1806(f), Plaintiffs must satisfy the definition of an "aggrieved person," *see id.* § 1801(k).

We addressed the "aggrieved person" requirement in part in the discussion of Plaintiffs' § 1810 claim against the Agent Defendants. As we there explained, because Fazaga had a reasonable expectation of privacy in his office, and AbdelRahim had a reasonable expectation of privacy in his home, car, and phone, Plaintiffs are properly considered aggrieved persons as to those categories of surveillance. *See supra* Part I.C. And although we noted that the Agent Defendants are entitled to qualified immunity on Plaintiffs' FISA § 1810 claim with respect to the recording of conversation in the mosque prayer halls, Plaintiffs had a reasonable expectation of privacy in those conversations and thus are still properly considered aggrieved persons as to that category of surveillance as well. *See supra* Part I.B.

Again, because Plaintiffs are properly considered "aggrieved" for purposes of FISA, two of the situations referenced in § 1806(f) are directly applicable here. The Government intends to use "information obtained or derived from an electronic surveillance" against Plaintiffs, who are "aggrieved person[s]." 50 U.S.C. § 1806(c). And Plaintiffs are "aggrieved person[s]" who have attempted "to discover or obtain applications or orders or other materials relating to electronic surveillance." *Id.* § 1806(f).

* * * *

We next turn to considering whether the claims other than the FISA § 1810 claim must be dismissed for rea-

sons independent of the state secrets privilege, limiting ourselves to the arguments for dismissal raised in Defendants' motions to dismiss.

III. Search Claims

In this part, we discuss (1) the Fourth Amendment injunctive relief claim against the official-capacity defendants; and (2) the Fourth Amendment *Bivens* claim against the Agent Defendants.

A. Fourth Amendment Injunctive Relief Claim Against the Official-Capacity Defendants

The Government's primary argument for dismissal of the constitutional claims brought against the official-capacity defendants, including the Fourth Amendment claim, is that the injunctive relief sought—the expungement of all records unconstitutionally obtained and maintained—is unavailable under the Constitution. Not so.

We have repeatedly and consistently recognized that federal courts can order expungement of records, criminal and otherwise, to vindicate constitutional rights.[32]

---

[32] *See, e.g.*, *United States v. Sumner*, 226 F.3d 1005, 1012 (9th Cir. 2000) ("A district court has the power to expunge a criminal record under . . . the Constitution itself."); *Burnsworth v. Gunderson*, 179 F.3d 771, 775 (9th Cir. 1999) (holding that expungement of an escape conviction from prison records was an appropriate remedy for a due process violation); *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1275 (9th Cir. 1998) (explaining that expungement of unconstitutionally obtained medical records "would be an appropriate remedy for the alleged violation"); *United States v. Smith*, 940 F.2d 395, 396 (9th Cir. 1991) (per curiam) (explaining that "recognized circumstances supporting expunction" include an unlawful or invalid arrest or conviction and government misconduct); *Fendler v. U.S. Parole Comm'n*, 774 F.2d 975, 979 (9th Cir. 1985) ("Federal courts have the equitable power 'to order the expungement of Gov-

The Privacy Act, 5 U.S.C. § 552a, which (1) establishes a set of practices governing the collection, maintenance, use, and dissemination of information about individuals maintained in records systems by federal agencies, and (2) creates federal claims for relief for violations of the Act's substantive provisions, does not displace the availability of expungement relief under the Constitution.[33] Previous cases involving claims brought under both the Privacy Act and the Constitution did not treat the Privacy Act as displacing a constitutional claim, but instead

---

ernment records where *necessary* to vindicate rights secured by the Constitution or by statute.'" (quoting *Chastain v. Kelley*, 510 F.2d 1232, 1235 (D.C. Cir. 1975))); *Maurer v. Pitchess*, 691 F.2d 434, 437 (9th Cir. 1982) ("It is well settled that the federal courts have inherent equitable power to order 'the expungement of local arrest records as an appropriate remedy in the wake of police action in violation of constitutional rights.'" (quoting *Sullivan v. Murphy*, 478 F.2d 938, 968 (D.C. Cir. 1973))); *Shipp v. Todd*, 568 F.2d 133, 134 (9th Cir. 1978) ("It is established that the federal courts have inherent power to expunge criminal records when necessary to preserve basic legal rights." (quoting *United States v. McMains*, 540 F.2d 387, 389 (8th Cir. 1976))).

[33] The cases cited by the Government to the contrary are inapposite. *See City of Milwaukee*, 451 U.S. at 314-16 (addressing the congressional displacement of federal common law through legislation, not the elimination of injunctive remedies available under the Constitution); *Bush v. Lucas*, 462 U.S. 367, 386-88 (1983) (discussing preclusion of a *Bivens* claim for damages where Congress had already designed a comprehensive remedial scheme, not whether a statute can displace a recognized constitutional claim for injunctive relief); *Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 936-37 (D.C. Cir. 2003) (discussing the displacement of a common law right of access to public records by the Freedom of Information Act in a case not involving the Privacy Act or a claim for injunctive relief from an alleged ongoing constitutional violation).

analyzed the claims separately.[34] And the circuits that have directly considered whether the Privacy Act displaces parallel constitutional remedies have all concluded that a plaintiff may pursue a remedy under both the Constitution and the Privacy Act.[35]

In addition to its Privacy Act displacement theory, the Government contends that even if expungement relief is otherwise available under the Constitution, it is not available here, as Plaintiffs "advance no plausible claim of an ongoing constitutional violation." Again, we disagree.

This court has been clear that a determination that records were obtained and retained in violation of the Constitution supports a claim for expungement relief of existing records so obtained. As *Norman-Bloodsaw* explained:

> Even if the continued storage, against plaintiffs' wishes, of intimate medical information that was allegedly taken from them by unconstitutional means

---

[34] *See Hewitt v. Grabicki*, 794 F.2d 1373, 1377, 1380 (9th Cir. 1986) (addressing separately a claim for damages under the Privacy Act and a procedural due process claim); *Fendler*, 774 F.2d at 979 (considering a prisoner's Privacy Act claims and then, separately, his claim for expungement relief under the Constitution).

[35] *See Abdelfattah v. U.S. Dep't of Homeland Sec.*, 787 F.3d 524, 534 (D.C. Cir. 2015) ("We have repeatedly recognized a plaintiff may request expungement of agency records for both violations of the Privacy Act and the Constitution."); *Clarkson v. IRS*, 678 F.2d 1368, 1376 n.13 (11th Cir. 1982) ("[W]e of course do not intend to suggest that the enactment of the Privacy Act in any way precludes a plaintiff from asserting a constitutional claim for violation of his privacy or First Amendment rights. Indeed, several courts have recognized that a plaintiff is free to assert both Privacy Act and constitutional claims.").

> does not *itself* constitute a violation of law, it is clearly an ongoing "effect" of the allegedly unconstitutional and discriminatory testing, and expungement of the test results would be an appropriate remedy for the alleged violation. . . . At the very least, the retention of undisputedly intimate medical information obtained in an unconstitutional and discriminatory manner would constitute a continuing "irreparable injury" for purposes of equitable relief.

135 F.3d at 1275; *see also Wilson v. Webster*, 467 F.2d 1282, 1283-84 (9th Cir. 1972) (holding that plaintiffs had a right to show that records of unlawful arrests "should be expunged, for their continued existence may seriously and unjustifiably serve to impair fundamental rights of the persons to whom they relate").

In short, expungement relief is available under the Constitution to remedy the alleged constitutional violations.[36] Because the Government raises no other argument for dismissal of the Fourth Amendment injunctive relief claim, it should not have been dismissed.

B. Fourth Amendment *Bivens* Claim Against the Agent Defendants

Alleging that the Agent Defendants violated the Fourth Amendment, Plaintiffs seek monetary damages directly under the Constitution under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971). In *Bivens*, the Supreme Court "recognized for the first time an implied private action for damages against federal officers alleged to have violated a citizen's constitutional rights." *Corr. Servs. Corp. v.*

---

[36] We do not at this stage, of course, address whether Plaintiffs are actually entitled to such a remedy.

Malesko, 534 U.S. 61, 66 (2001). "The purpose of *Bivens* is to deter individual federal officers from committing constitutional violations." *Id.* at 70.

Bivens itself concerned a Fourth Amendment violation by federal officers. As we have recognized, a Fourth Amendment damages claim premised on unauthorized electronic surveillance by FBI agents and their surrogates "fall[s] directly within the coverage of *Bivens*." *Gibson v. United States*, 781 F.2d 1334, 1341 (9th Cir. 1986); *see also Mitchell v. Forsyth*, 472 U.S. 511, 513 (1985) (considering, under *Bivens*, an alleged "warrantless wiretap" conducted in violation of the Fourth Amendment). Recent cases, however, have severely restricted the availability of *Bivens* actions for new claims and contexts. *See Ziglar v. Abbasi*, 137 S. Ct. 1843, 1856-57 (2017).[37]

Here, the substance of Plaintiffs' Fourth Amendment *Bivens* claim is identical to the allegations raised in their FISA § 1810 claim. Under our rulings regarding the reach of the § 1806(f) procedures, almost all of the search-and-seizure allegations will be subject to those procedures. Thus, regardless of whether a *Bivens* remedy is available, Plaintiffs' underlying claim—that the Agent Defendants engaged in unlawful electronic surveillance violative of the Fourth Amendment—would proceed in the same way.

Moreover, if the Fourth Amendment *Bivens* claim proceeds, the Agent Defendants are entitled to qualified immunity on Plaintiffs' Fourth Amendment *Bivens* claim to the same extent they are entitled to qualified

---

[37] The parties have not briefed before us the impact of *Abbasi* on the *Bivens* claims.

immunity on Plaintiffs' FISA claim. In both instances, the substantive law derives from the Fourth Amendment, and in both instances, government officials in their individual capacity are subject to liability for damages only if they violated a clearly established right to freedom from governmental intrusion where an individual has a reasonable expectation of privacy. *See supra* Part I.B. Under our earlier rulings, the FISA search-and-seizure allegations may proceed against only two of the Agent Defendants, and only with respect to a narrow aspect of the alleged surveillance.

In light of the overlap between the *Bivens* claim and the narrow range of the remaining FISA claim against the Agent Defendants that can proceed, it is far from clear that Plaintiffs will continue to press this claim. We therefore decline to address whether Plaintiffs' *Bivens* claim remains available after the Supreme Court's decision in *Abbasi*. On remand, the district court may determine—if necessary—whether a *Bivens* remedy is appropriate for any Fourth Amendment claim against the Agent Defendants.

IV. Religion Claims

The other set of Plaintiffs' claims arise from their allegation that they were targeted for surveillance solely because of their religion.[38] In this part, we discuss Plaintiffs' (1) First and Fifth Amendment injunctive relief claims against the official-capacity defendants; (2) First and Fifth Amendment *Bivens* claims against the Agent Defendants; (3) § 1985(3) claims for violations of

---

[38] The operative complaint alleges as a factual matter that Plaintiffs were surveilled solely because of their religion. We limit our legal discussion to the facts there alleged.

the Free Exercise Clause, Establishment Clause, and equal protection guarantee; (4) RFRA claim; (5) Privacy Act claim; and (6) FTCA claims. Our focus throughout is whether there are grounds for dismissal independent of the Government's invocation of the state secrets privilege.

A. First Amendment and Fifth Amendment Injunctive Relief Claims Against the Official-Capacity Defendants

Plaintiffs maintain that it violates the First Amendment's Religion Clauses and the equal protection component of the Fifth Amendment for the Government to target them for surveillance because of their adherence to and practice of Islam. The Government does not challenge the First and Fifth Amendment claims substantively. It argues only that injunctive relief is unavailable and that litigating the claims is not possible without risking the disclosure of state secrets. We have already concluded that injunctive relief, including expungement, is available under the Constitution where there is a substantively viable challenge to government action, *see supra* Part III.A, and that dismissal because of the state secrets concern was improper because of the availability of the § 1806(f) procedures, *see supra* Part II. Accordingly, considering only the arguments put forward by the Government, we conclude that the First and Fifth Amendment claims against the official-capacity defendants may go forward.

B. First Amendment and Fifth Amendment *Bivens* Claims Against the Agent Defendants

Plaintiffs seek monetary damages directly under the First Amendment's Establishment and Free Exercise Clauses and the equal protection component of the Fifth

Amendment's Due Process Clause, relying on *Bivens v. Six Unknown Named Agents*.

We will not recognize a *Bivens* claim where there is "'any alternative, existing process for protecting' the plaintiff's interests." *W. Radio Servs. Co. v. U.S. Forest Serv.*, 578 F.3d 1116, 1120 (9th Cir. 2009) (quoting *Wilkie v. Robbins*, 551 U.S. 537, 550 (2007)). The existence of such an alternative remedy raises the inference that Congress "'expected the Judiciary to stay its *Bivens* hand' and 'refrain from providing a new and freestanding remedy in damages.'" *Id.* (quoting *Wilkie*, 551 U.S. at 550, 554); *see also Abbasi*, 137 S. Ct. at 1863; *Schweiker v. Chilicky*, 487 U.S. 412, 423 (1988). Accordingly, we "refrain[] from creating a judicially implied remedy even when the available statutory remedies 'do not provide complete relief' for a plaintiff that has suffered a constitutional violation." *W. Radio Servs.*, 578 F.3d at 1120 (quoting *Malesko*, 534 U.S. at 69). As long as "an avenue for some redress" exists, "bedrock principles of separation of powers forclose[s] judicial imposition of a new substantive liability.'" *Id.* (alteration in original) (quoting *Malesko*, 534 U.S. at 69).

Here, we conclude that the Privacy Act, 5 U.S.C. § 552a, and the Religious Freedom Restoration Act, 42 U.S.C. § 2000bb *et seq.*, taken together, provide an alternative remedial scheme for some, but not all, of Plaintiffs' First and Fifth Amendment *Bivens* claims. As to the remaining *Bivens* claims, we remand to the district court to decide whether a *Bivens* remedy is available in light of the Supreme Court's decision in *Abbasi*.

As to the collection and maintenance of records, Plaintiffs could have, and indeed did, challenge the FBI's surveillance of them under the Privacy Act's re-

medial scheme. Again, the Privacy Act, 5 U.S.C. § 552a, creates a set of rules governing how such records should be kept by federal agencies. *See supra* Part III.A. Under § 552a(e)(7), an "agency that maintains a system of records shall maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[39] When an agency fails to comply with § 552a(e)(7), an individual may bring a civil action against the agency for damages. *Id.* § 552a(g)(1)(D), (g)(4). Thus, § 552a(e)(7) limits the government's ability to collect, maintain, use, or disseminate information on an individual's religious activity protected by the First Amendment's Religion Clauses.

We have not addressed the availability of a *Bivens* action where the Privacy Act may be applicable. But two other circuits have, and both held that the Privacy Act supplants *Bivens* claims for First and Fifth Amendment violations. *See Wilson v. Libby*, 535 F.3d 697, 707-08 (D.C. Cir. 2008) (holding, in response to claims alleging harm from the improper disclosure of information subject to the Privacy Act's protections, that the Privacy Act is a comprehensive remedial scheme that precludes an additional *Bivens* remedy); *Downie v. City of Middleburg Heights*, 301 F.3d 688, 696 & n.7 (6th Cir. 2002) (holding that the Privacy Act displaces *Bivens* for claims involving the creation, maintenance, and dissemination of false records by federal agency employees). We agree with the analyses in *Wilson* and *Downie*.

---

[39] The term "maintain" is defined to mean "maintain, collect, use, or disseminate." 5 U.S.C. § 552a(a)(3).

Although the Privacy Act provides a remedy only against the FBI, not the individual federal officers, the lack of relief against some potential defendants does not disqualify the Privacy Act as an alternative remedial scheme. Again, a *Bivens* remedy may be foreclosed "even when the available statutory remedies 'do not provide complete relief' for a plaintiff," as long as "the plaintiff ha[s] an avenue for *some* redress." *W. Radio Servs.*, 578 F.3d at 1120 (alteration in original) (emphasis added) (quoting *Malesko*, 534 U.S. at 69). Thus, to the extent that Plaintiffs' *Bivens* claims involve improper collection and retention of agency records, the Privacy Act precludes such *Bivens* claims.

As to religious discrimination more generally, we conclude that RFRA precludes some, but not all, of Plaintiffs' *Bivens* claims. RFRA provides that absent a "compelling governmental interest" and narrow tailoring, 42 U.S.C. § 2000bb-1(b), the "Government shall not substantially burden a person's exercise of religion even if the burden results from a rule of general applicability." *Id.* § 2000bb-1(a). The statute was enacted "to provide a claim or defense to persons whose religious exercise is substantially burdened by government." *Id.* § 2000bb(b)(2). It therefore provided that "[a] person whose religious exercise has been burdened in violation of this section may assert that violation as a claim or defense in a judicial proceeding and obtain appropriate relief against a government." *Id.* § 2000bb-1(c). RFRA thus provides a means for Plaintiffs to seek relief for the alleged burden of the surveillance itself on their exercise of their religion.

RFRA does not, however, provide an alternative remedial scheme for all of Plaintiffs' discrimination-based

Bivens claims. RFRA was enacted in response to *Employment Division v. Smith*, 494 U.S. 872 (1990), which, in Congress's view, "virtually eliminated the requirement that the government justify burdens on religious exercise imposed by laws neutral toward religion," 42 U.S.C. § 2000bb(a)(4). Accordingly, "to restore the compelling interest test . . . and to guarantee its application in all cases where free exercise of religion is substantially burdened," *id.* § 2000bb(b)(1), RFRA directs its focus on "rule[s] of general applicability" that "substantially burden a person's exercise of religion," *id.* § 2000bb-1(a).

Here, many of Plaintiffs' allegations relate not to neutral and generally applicable government action, but to conduct motivated by intentional discrimination against Plaintiffs because of their Muslim faith. Regardless of the magnitude of the burden imposed, "if the object of a law is to infringe upon or restrict practices *because* of their religious motivation, the law is not neutral" and "is invalid unless it is justified by a compelling interest and is narrowly tailored to advance that interest." *Church of the Lukumi Babalu Aye, Inc. v. City of Hialeah*, 508 U.S. 520, 533 (1993) (emphasis added). It is the Free Exercise Clause of the First Amendment—not RFRA—that imposes this requirement.

Moreover, by its terms, RFRA applies only to the "free exercise of religion," 42 U.S.C. § 2000bb(a)(1); indeed, it expressly disclaims any effect on "that portion of the First Amendment prohibiting laws respecting the establishment of religion," *id.* § 2000bb-4. But intentional religious discrimination is "subject to heightened scrutiny whether [it] arise[s] under the Free Exercise Clause, the Establishment Clause, or the Equal Protec-

tion Clause." *Colo. Christian Univ. v. Weaver*, 534 F.3d 1245, 1266 (10th Cir. 2008) (citations omitted). Here, Plaintiffs have raised religion claims based on all three constitutional provisions. Because RFRA does not provide an alternative remedial scheme for protecting these interests, we conclude that RFRA does not preclude Plaintiffs' religion-based *Bivens* claims.

We conclude that the Privacy Act and RFRA, taken together, function as an alternative remedial scheme for protecting some, but not all, of the interests Plaintiffs seek to vindicate via their First and Fifth Amendment *Bivens* claims. The district court never addressed whether a *Bivens* remedy is available for any of the religion claims because it dismissed the claims in their entirety based on the state secrets privilege. In addition, *Abbasi* has now clarified the standard for determining when a *Bivens* remedy is available for a particular alleged constitutional violation. And, as we have explained, the scope of the religion claims to which a *Bivens* remedy might apply is considerably narrower than those alleged, given the partial displacement by the Privacy Act and RFRA. If asked, the district court should determine on remand, applying *Abbasi*, whether a *Bivens* remedy is available to the degree the damages remedy is not displaced by the Privacy Act and RFRA.

C. 42 U.S.C. § 1985(3) Claims Against the Agent Defendants

Plaintiffs allege that the Agent Defendants conspired to deprive Plaintiffs of their rights under the First Amendment's Establishment and Free Exercise Clauses and the due process guarantee of the Fifth Amendment, in violation of 42 U.S.C. § 1985(3).

To state a violation of § 1985(3), Plaintiffs must "allege and prove four elements":

> (1) a conspiracy; (2) for the purpose of depriving, either directly or indirectly, any person or class of persons of the equal protection of the laws, or of equal privileges and immunities under the laws; and (3) an act in furtherance of the conspiracy; (4) whereby a person is either injured in his person or property or deprived of any right or privilege of a citizen of the United States.

United Bhd. of Carpenters & Joiners of Am., Local 610 v. Scott, 463 U.S. 825, 828-29 (1983). The Defendants attack these claims on various grounds, but we reach only one—whether § 1985(3) conspiracies among employees of the same government entity are barred by the intracorporate conspiracy doctrine.

Abbasi makes clear that intracorporate liability was not clearly established at the time of the events in this case and that the Agent Defendants are therefore entitled to qualified immunity from liability under § 1985(3). *See* 137 S. Ct. at 1866.

In *Abbasi*, men of Arab and South Asian descent detained in the aftermath of September 11 sued two wardens of the federal detention center in Brooklyn in which they were held, along with several high-level Executive Branch officials who were alleged to have authorized their detention. *Id.* at 1853. They alleged, among other claims, a conspiracy among the defendants to deprive them of the equal protection of the laws under § 1985(3).[40] *Id.* at 1853-54. *Abbasi* held that, even as-

[40] Specifically, Plaintiffs alleged that these officials "conspired with one another to hold respondents in harsh conditions because of

suming these allegations to be "true and well pleaded," the defendants were entitled to qualified immunity on the § 1985(3) claim. *Id.* at 1866-67. It was not "clearly established" at the time, the Court held, that the intracorporate conspiracy doctrine did not bar § 1985(3) liability for employees of the same government department who conspired among themselves. *Id.* at 1867-68. "[T]he fact that the courts are divided as to whether or not a § 1985(3) conspiracy can arise from official discussions between or among agents of the same entity demonstrates that the law on the point is not well established." *Id.* at 1868. "[R]easonable officials in petitioners' positions would not have known, and could not have predicted, that § 1985(3) prohibited their joint consultations." *Id.* at 1867. The Court declined, however, to resolve the issue on the merits. *Id.*

Abbasi controls. Although the underlying facts here differ from those in *Abbasi*, the dispositive issue here, as in *Abbasi*, is whether the Agent Defendants could reasonably have known that agreements entered into or agreed-upon policies devised with other employees of the FBI could subject them to conspiracy liability under § 1985(3). At the time Plaintiffs allege they were surveilled, neither this court nor the Supreme Court had held that an intracorporate agreement could subject federal officials to liability under § 1985(3), and the circuits that had decided the issue were split.[41] There was

---

their actual or apparent race, religion, or national origin." *Abbasi*, 137 S. Ct. at 1854.

[41] Two circuits have held that the intracorporate conspiracy doctrine does not extend to civil rights cases. *See Brever v. Rockwell Int'l Corp.*, 40 F.3d 1119, 1127 (10th Cir. 1994); *Novotny v. Great Am. Fed. Sav. & Loan Ass'n*, 584 F.2d 1235, 1257-58 (3d Cir. 1978) (en banc), *vacated on other grounds*, 442 U.S. 366 (1979); *see also*

therefore, as in *Abbasi*, no clearly established law on the question. As the Agent Defendants are entitled to qualified immunity on the § 1985(3) allegations in the complaint, we affirm their dismissal on that ground.

D. Religious Freedom Restoration Act Claim Against the Agent Defendants and Government Defendants

Plaintiffs allege that the Defendants violated the Religious Freedom Restoration Act, 42 U.S.C. § 2000bb, by substantially burdening Plaintiffs' exercise of religion, and did so neither in furtherance of a compelling governmental interest nor by adopting the least restrictive means of furthering any such interest. The Government Defendants offer no argument for dismissal of the RFRA claim other than the state secrets privilege. The Agent Defendants, however, contend that they are entitled to qualified immunity on the RFRA claim because Plaintiffs failed to plead a substantial burden on their religion, and if they did so plead, no clearly established law supported that conclusion at the relevant time.[42]

Stathos v. Bowden, 728 F.2d 15, 20-21 (1st Cir. 1984) (expressing "doubt" that the intracorporate conspiracy doctrine extends to conspiracy under § 1985(3)). The majority of the circuits have reached a contrary result. *See Hartline v. Gallo*, 546 F.3d 95, 99 n.3 (2d Cir. 2008); *Meyers v. Starke*, 420 F.3d 738, 742 (8th Cir. 2005); *Dickerson v. Alachua Cty. Comm'n*, 200 F.3d 761, 767-68 (11th Cir. 2000); *Benningfield v. City of Houston*, 157 F.3d 369, 378 (5th Cir. 1998); *Wright v. Ill. Dep't of Children & Family Servs.*, 40 F.3d 1492, 1508 (7th Cir. 1994); *Hull v. Cuyahoga Valley Joint Vocational Sch. Dist. Bd. of Educ.*, 926 F.2d 505, 509-10 (6th Cir. 1991); *Buschi v. Kirven*, 775 F.2d 1240, 1252-53 (4th Cir. 1985).

[42] The parties do not dispute that qualified immunity is an available defense to a RFRA claim. We therefore assume it is. *See Padilla*

To establish a prima facie claim under RFRA, a plaintiff must "present evidence sufficient to allow a trier of fact rationally to find the existence of two elements." *Navajo Nation v. U.S. Forest Serv.*, 535 F.3d 1058, 1068 (9th Cir. 2008) (en banc). "First, the activities the plaintiff claims are burdened by the government action must be an 'exercise of religion.'" *Id.* (quoting 42 U.S.C. § 2000bb-1(a)). "Second, the government action must 'substantially burden' the plaintiff's exercise of religion." *Id.* Once a plaintiff has established those elements, "the burden of persuasion shifts to the government to prove that the challenged government action is in furtherance of a 'compelling governmental interest' and is implemented by 'the least restrictive means.'" *Id.* (quoting 42 U.S.C. § 2000bb-1(b)).

"Under RFRA, a 'substantial burden' is imposed only when individuals are forced to choose between following the tenets of their religion and receiving a governmental benefit . . . or coerced to act contrary to their religious beliefs by the threat of civil or criminal sanctions. . . . " *Id.* at 1069-70; *see also Oklevueha Native Am. Church of Haw., Inc. v. Lynch*, 828 F.3d 1012, 1016 (9th Cir. 2016). An effect on an individual's "subjective, emotional religious experience" does not constitute a

---

v. Yoo, 678 F.3d 748, 768 (9th Cir. 2012); *Lebron v. Rumsfeld*, 670 F.3d 540, 560 (4th Cir. 2012).

Tidwell and Walls also contend that Plaintiffs' RFRA claim was properly dismissed because RFRA does not permit damages suits against individual-capacity defendants. Because we affirm dismissal on another ground, we do not reach that issue. We note, however, that at least two other circuits have held that damages are available for RFRA suits against individual-capacity defendants. *See Tanvir v. Tanzin*, 894 F.3d 449, 467 (2d Cir. 2018); *Mack v. Warden Loretto FCI*, 839 F.3d 286, 302 (3d Cir. 2016).

substantial burden, *Navajo Nation*, 535 F.3d at 1070, nor does "a government action that decreases the spirituality, the fervor, or the satisfaction with which a believer practices his religion," *id.* at 1063.

Plaintiffs do allege that they altered their religious practices as a result of the FBI's surveillance: Malik trimmed his beard, stopped regularly wearing a skull cap, decreased his attendance at the mosque, and became less welcoming to newcomers than he believes his religion requires. AbdelRahim "significantly decreased his attendance to mosque," limited his donations to mosque institutions, and became less welcoming to newcomers than he believes his religion requires. Fazaga, who provided counseling at the mosque as an imam and an intern therapist, stopped counseling congregants at the mosque because he feared the conversations would be monitored and thus not confidential.

But it was not clearly established in 2006 or 2007 that covert surveillance conducted on the basis of religion would meet the RFRA standards for constituting a substantial religious burden on individual congregants. There simply was no case law in 2006 or 2007 that would have put the Agent Defendants on notice that covert surveillance on the basis of religion could violate RFRA. And at least two cases from our circuit could be read to point in the opposite direction, though they were brought under the First Amendment's Religion Clauses rather than under RFRA. *See Vernon v. City of Los Angeles*, 27 F.3d 1385, 1394 (9th Cir. 1994); *Presbyterian Church*, 870 F.2d at 527.[43]

---

[43] *Presbyterian Church* predates *Employment Division v. Smith*, which declined to use the compelling interest test from *Sherbert v.*

Presbyterian Church concerned an undercover investigation by INS of the sanctuary movement. 870 F.2d at 520. Over nearly a year, several INS agents infiltrated four churches in Arizona, attending and secretly recording church services. *Id.* The covert surveillance was later publicly disclosed in the course of criminal proceedings against individuals involved with the sanctuary movement. *Id.* The four churches brought suit, alleging a violation of their right to free exercise of religion. *Id.* We held that the individual INS agents named as defendants were entitled to qualified immunity because there was "no support in the preexisting case law" to suggest that "it must have been apparent to INS officials that undercover electronic surveillance of church services without a warrant and without probable cause violated the churches' clearly established rights under the First . . . Amendment[]." *Id.* at 527.

In *Vernon*, the Los Angeles Police Department ("LAPD") investigated Vernon, the Assistant Chief of Police of the LAPD, in response to allegations that Vernon's religious beliefs had interfered with his ability or willingness to fairly perform his official duties. 27 F.3d at 1389. Vernon filed a § 1983 action, maintaining that the preinvestigation activities and the investigation itself violated the Free Exercise Clause. *Id.* at 1390. In

---

Verner, 374 U.S. 398 (1963). *Smith*, 494 U.S. at 883-85. The other case, *Vernon*, postdates RFRA, which in 1993 restored *Sherbert*'s compelling interest test. *See* 27 F.3d at 1393 n.1; *see also* 42 U.S.C. § 2000bb(b). Although the compelling interest balancing test was in flux during this period, the notion that a burden on religious practice was required to state a claim was not. RFRA continued the same substantial burden standard as was required by the constitutional cases. *See Vernon*, 27 F.3d at 1393.

his complaint, Vernon alleged that the investigation "chilled [him] in the exercise of his religious beliefs, fearing that he can no longer worship as he chooses, consult with his ministers and the elders of his church, participate in Christian fellowship and give public testimony to his faith without severe consequences." *Id.* at 1394. We held that Vernon failed to demonstrate a substantial burden on his religious observance and so affirmed the district court's dismissal of his free exercise claim. *Id.* at 1395. We noted that Vernon "failed to show any concrete and demonstrable injury." *Id.* "Vernon complain[ed] that the existence of a government investigation has discouraged him from pursuing his personal religious beliefs and practices—in other words, mere subjective chilling effects with neither 'a claim of specific present objective harm [n]or a threat of specific future harm.'" *Id.* (quoting *Laird v. Tatum*, 408 U.S. 1, 14 (1972)).

Vernon and *Presbyterian Church* were decided before the surveillance Plaintiffs allege substantially burdened their exercise of religion. Both cases cast doubt upon whether surveillance such as that alleged here constitutes a substantial burden upon religious practice. There is no pertinent case law indicating otherwise. It was therefore not clearly established in 2006 or 2007 that Defendants' actions violated Plaintiffs' freedom of religion, protected by RFRA.[44]

---

[44] These cases may not, however, entitle the Agent Defendants to qualified immunity as to claims involving *intentional* discrimination based on Plaintiffs' religion. As we noted, *see supra* Part IV.B, we are not deciding whether there is an available *Bivens* action for those claims. As we decline to anticipate whether Plaintiffs will pursue their *Bivens* claims on the religious discrimination issues and, if so,

As to the Agent Defendants, therefore, we affirm the dismissal of the RFRA claim. But because the Government Defendants are not subject to the same qualified immunity analysis and made no arguments in support of dismissing the RFRA claim other than the state secrets privilege, we hold that the complaint substantively states a RFRA claim against the Government Defendants.[45]

E. Privacy Act Claim Against the FBI

Plaintiffs allege that the FBI violated the Privacy Act, 5 U.S.C. § 552a(e)(7),[46] by collecting and maintaining records describing how Plaintiffs exercised their First Amendment rights. As a remedy, Plaintiffs seek only injunctive relief ordering the destruction or return of unlawfully obtained information. *Cell Associates, Inc. v. National Institutes of Health*, 579 F.2d 1155 (9th Cir. 1978), which interpreted the scope of Privacy Act remedies, precludes such injunctive relief.

The "Civil remedies" section of the Privacy Act, 5 U.S.C. § 552a(g), lists four types of agency misconduct and the remedies applicable to each. The statute ex-

---

whether the claims will be allowed to go forward, we leave any surviving qualified immunity issue for the district court to decide in the first instance.

[45] We do not address any other defenses the Government Defendants may raise before the district court in response to Plaintiffs' RFRA claim.

[46] The header to Plaintiffs' Eighth Cause of Action reads broadly, "Violation of the Privacy Act, 5 U.S.C. § 552a(a)-(*l*)." As actually pleaded and briefed, however, the substance of Plaintiffs' Privacy Act claim is limited to § 552a(e)(7). The complaint states that "Defendant FBI . . . collected and maintained records . . . in violation of 5 U.S.C. § 552a(e)(7)." And Plaintiffs' reply brief states that they "seek expungement . . . under 5 U.S.C. § 552a(e)(7)."

pressly provides that injunctive relief is available when an agency improperly denies a request to amend or disclose an individual's record, *see* 5 U.S.C. § 552a(g)(1)(A), (2)(A), (1)(B), (3)(A), but provides only for damages when the agency "fails to maintain any record" with the "accuracy, relevance, timeliness, and completeness" required for fairness, *id.* § 552a(g)(1)(C), or if the agency "fails to comply with any other provision" of the Privacy Act, *id.* § 552a(g)(1)(D). *See id.* § 552a(g)(4). *Cell Associates* concluded that this distinction was purposeful — that is, that Congress intended to limit the availability of injunctive relief to the categories of agency misconduct for which injunctive relief was specified as a remedy:

> The addition of a right to injunctive relief for one type of violation, coupled with the failure to provide injunctive relief for another type of violation, suggests that Congress knew what it was about and intended the remedies specified in the Act to be exclusive. While the right to damages might seem an inadequate safeguard against unwarranted disclosures of agency records, we think it plain that Congress limited injunctive relief to the situations described in 5 U.S.C. § 552a(g)(1)(A) and (2) and (1)(B) and (3).

579 F.2d at 1161.

A violation of § 552a(e)(7) falls within the catch-all remedy provision, applicable if the agency "fails to comply with any other provision" of the Privacy Act. 5 U.S.C. § 552a(g)(1)(D). As the statute does not expressly provide for injunctive relief for a violation of this catch-all provision, *Cell Associates* precludes injunctive relief for a violation of § 552a(e)(7).

Plaintiffs attempt to avoid the precedential impact of *Cell Associates* on the ground that it "nowhere mentions Section 552a(e)(7)." That is so, but the holding of *Cell Associates* nonetheless applies directly to this case. The Privacy Act specifies that injunctive relief *is* available for violations of some provisions of the Act, but not for a violation of § 552a(e)(7). Under *Cell Associates*, Plaintiffs cannot obtain injunctive relief except for violations as to which such relief is specifically permitted.[47]

Plaintiffs' complaint expressly provides that "[t]he FBI is sued for injunctive relief only." Accordingly, because their sole requested remedy is unavailable, Plaintiffs fail to state a claim under the Privacy Act.

F. FTCA Claims

The FTCA constitutes a waiver of sovereign immunity "under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred." 28 U.S.C. § 1346(b)(1). "State substantive law applies" in FTCA actions. *Liebsack v. United States*, 731 F.3d 850, 856 (9th Cir. 2013). If an individual federal employee is sued, the United States shall, given certain conditions are satisfied, "be substituted as the party defendant." 28 U.S.C. § 2679(d)(1).

Plaintiffs allege that the United States is liable under the FTCA for invasion of privacy under California law,

---

[47] Plaintiffs also argue that *MacPherson v. IRS*, 803 F.2d 479 (9th Cir. 1986) is "binding Ninth Circuit authority . . . [that] makes clear that courts have authority to order expungement of records maintained in violation of its [§ 552a(e)(7)] requirements." But *MacPherson* does not state whether the plaintiff there sought injunctive relief and so is unclear on this point.

violation of the California constitutional right to privacy, violation of California Civil Code § 52.1, and intentional infliction of emotional distress. We first consider Defendants' jurisdictional arguments, and then discuss their implications for the substantive FTCA claims.

1. FTCA Judgment Bar

The FTCA's judgment bar provides that "[t]he judgment in an action under [the FTCA] shall constitute a complete bar to any action by the claimant, by reason of the same subject matter, against the employee of the government whose act or omission gave rise to the claim." 28 U.S.C. § 2676. The judgment bar provision has no application here.

The judgment bar provision precludes claims against individual defendants in two circumstances: (1) where a plaintiff brings an FTCA claim against the government and non-FTCA claims against individual defendants in the same action and obtains a judgment against the government, *see Kreines v. United States*, 959 F.2d 834, 838 (9th Cir. 1992); and (2) where the plaintiff brings an FTCA claim against the government, judgment is entered in favor of either party, and the plaintiff then brings a subsequent non-FTCA action against individual defendants, *see Gasho v. United States*, 39 F.3d 1420, 1437-38 (9th Cir. 1994); *Ting v. United States*, 927 F.2d 1504, 1513 n.10 (9th Cir. 1991). The purposes of this judgment bar are "to prevent dual recoveries," *Kreines*, 959 F.2d at 838, to "serve[] the interests of judicial economy," and to "foster more efficient settlement of claims," by "encourag[ing plaintiffs] to pursue their claims concurrently in the same action, instead of in separate actions," *Gasho*, 39 F.3d at 1438.

Neither of those two circumstances, nor their attendant risks, is present here. Plaintiffs brought their FTCA claim, necessarily, against the United States, and their non-FTCA claims against the Agent Defendants, in the same action. They have not obtained a judgment against the government. *Kreines* held that "an FTCA judgment in favor of the government did not bar the *Bivens* claim [against individual employees] when the judgments are 'contemporaneous' and part of the same action." *Gasho*, 39 F.3d at 1437 (quoting *Kreines*, 959 F.2d at 838). By "contemporaneous," *Kreines* did not require that judgments on the FTCA and other claims be entered simultaneously, but rather that they result from the same action.

The FTCA's judgment bar does not operate to preclude Plaintiffs' claims against the Agent Defendants.

2. FTCA Discretionary Function Exception

The discretionary function exception provides that the FTCA shall not apply to "[a]ny claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation, . . . or based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused." 28 U.S.C. § 2680(a). "[T]he discretionary function exception will not apply when a federal statute, regulation, or policy specifically prescribes a course of action for an employee to follow." *Berkovitz v. United States*, 486 U.S. 531, 536 (1988). "[G]overnmental conduct cannot be discretionary if it violates a legal mandate." *Galvin v. Hay*, 374 F.3d 739, 758 (9th Cir. 2004) (quoting *Nurse v. United States*, 226 F.3d 996,

1002 (9th Cir. 2000)). Moreover, "the Constitution can limit the discretion of federal officials such that the FTCA's discretionary function exception will not apply." *Id.* (quoting *Nurse*, 226 F.3d at 1002 n.2).

We cannot determine the applicability of the discretionary function exception at this stage in the litigation. If, on remand, the district court determines that Defendants did not violate any federal constitutional or statutory directives, the discretionary function exception will bar Plaintiffs' FTCA claims.[48] But if the district court instead determines that Defendants did violate a nondiscretionary federal constitutional or statutory directive, the FTCA claims may be able to proceed to that degree.

Because applicability of the discretionary function will largely turn on the district court's ultimate resolution of the merits of Plaintiffs' various federal constitutional and statutory claims, discussing whether Plaintiffs substantively state claims as to the state laws underlying the FTCA claim would be premature. We therefore decline to do so at this juncture.

V. Procedures on Remand

On remand, the FISA and Fourth Amendment claims, to the extent we have held they are validly pleaded in the complaint and not subject to qualified immunity, should proceed as usual. *See supra* Part II.B. In light of our conclusion regarding the reach of FISA § 1806(f), the district court should, using § 1806(f)'s *ex parte* and *in camera* procedures, review any "materi-

---

[48] We note that the judgment bar, 28 U.S.C. § 2676, does not apply to FTCA claims dismissed under the discretionary function exception. *See Simmons v. Himmelreich*, 136 S. Ct. 1843, 1847-48 (2016).

als relating to the surveillance as may be necessary," 50 U.S.C. § 1806(f), including the evidence over which the Attorney General asserted the state secrets privilege, to determine whether the electronic surveillance was lawfully authorized and conducted. That determination will include, to the extent we have concluded that the complaint states a claim regarding each such provision, whether Defendants violated any of the constitutional and statutory provisions asserted by Plaintiffs in their complaint. As permitted by Congress, "[i]n making this determination, the court may disclose to [plaintiffs], under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.*[49]

The Government suggests that Plaintiffs' religion claims cannot be resolved using the § 1806(f) procedures because, as the district court found, "the central subject matter [of the case] is Operation Flex, a group of counterterrorism investigations that extend well beyond the purview of electronic surveillance." Although the larger *factual* context of the case involves more than electronic surveillance, a careful review of the "Claims for Relief" section of the complaint convinces us that all of Plaintiffs' *legal* causes of action relate to electronic surveil-

---

[49] Our circuit has not addressed the applicable standard for reviewing the district court's decision not to disclose FISA materials. Other circuits, however, have adopted an abuse of discretion standard. *See United States v. Ali*, 799 F.3d 1008, 1022 (8th Cir. 2015); *United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982).

lance, at least for the most part, and in nearly all instances entirely, and thus require a determination as to the lawfulness of the surveillance. Moreover, § 1806(f) provides that the district court may consider "other materials *relating* to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted," thereby providing for consideration of all parties' factual submissions and legal contentions regarding the background of the surveillance. *Id.* (emphasis added).

We did explain in Part I, *supra*, that not all of the surveillance detailed in the complaint as the basis for Plaintiffs' legal claims constitutes electronic surveillance as defined by FISA. *See id.* § 1801(k). Also, two of Plaintiffs' causes of action can be read to encompass more conduct than just electronic surveillance. Plaintiffs' RFRA claim, their Fifth Cause of Action, is not limited to electronic surveillance. Plaintiffs broadly allege that "[t]he actions of Defendants substantially burdened [their] exercise of religion." The FTCA claim for intentional infliction of emotional distress, the Eleventh Cause of Action, is also more broadly pleaded. It is far from clear, however, that as actually litigated, either claim will involve more than the electronic surveillance that is otherwise the focus of the lawsuit.[50]

---

[50] For example, whether the official-capacity defendants targeted Plaintiffs for surveillance in violation of the First Amendment will in all likelihood be proven or defended against using the same set of evidence regardless of whether the court considers the claim in terms of electronic surveillance in the mosque prayer hall or conversations to which Monteilh was a party.

At this stage, it appears that, once the district court uses § 1806(f)'s procedures to review the state secrets evidence *in camera* and *ex parte* to determine the lawfulness of that surveillance, it could rely on its assessment of the same evidence—taking care to avoid its public disclosure—to determine the lawfulness of the surveillance falling outside FISA's purview, should Plaintiffs wish to proceed with their claims as applied to that set of activity. Once the sensitive information has been considered *in camera* and *ex parte*, the small risk of disclosure—a risk Congress thought too small to preclude careful *ex parte*, *in camera* consideration by a federal judge—has already been incurred. The scope of the state secrets privilege "is limited by its underlying purpose." *Halpern v. United States*, 258 F.2d 36, 44 (2d Cir. 1958) (quoting *Roviaro v. United States*, 353 U.S. 53, 60 (1957)). It would stretch the privilege beyond its purpose to require the district court to consider the state secrets evidence *in camera* and *ex parte* for one claim, but then, when considering another claim, ignore the evidence and dismiss the claim even though it involves the exact same set of parties, facts, and alleged legal violations.

Should our prediction of the overlap between the information to be reviewed under the FISA procedures to determine the validity of FISA-covered electronic surveillance and the information pertinent to other aspects of the religion claims prove inaccurate, or should the FISA-covered electronic surveillance drop out of consideration,[51] the Government is free to interpose a specifically tailored, properly raised state secrets privilege de-

---

[51] As could happen if, for instance, Plaintiffs are unable to substantiate their factual allegations as to the occurrence of the surveillance.

fense. Should the Government do so, at that point the district court should consider anew whether "simply excluding or otherwise walling off the privileged information may suffice to protect the state secrets," *Jeppesen*, 614 F.3d at 1082, or whether dismissal is required because "the privilege deprives the defendant[s] of information that would otherwise give the defendant[s] a valid defense to the claim[s]," *id.* at 1083 (quoting *Kasza*, 133 F.3d at 1166), or because the privileged and nonprivileged evidence are "inseparable" such that "litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets," *id.*

Because *Jeppesen* did not define "valid defense," we briefly address its meaning, so as to provide guidance to the district court on remand and to future courts in our circuit addressing the implications of the Government's invocation of the state secrets privilege.

The most useful discussion of the meaning of "valid defense" in the state secrets context is in the D.C. Circuit's decision in *In re Sealed Case*, 494 F.3d 139, cited by *Jeppensen*, 614 F.3d at 1083. We find the D.C. Circuit's definition and reasoning persuasive, and so adopt it. Critically, *In re Sealed Case* explained that "[a] 'valid defense' . . . is meritorious and not merely plausible and would require judgment for the defendant." 494 F.3d at 149. The state secrets privilege does not require "dismissal of a complaint for any plausible or colorable defense." *Id.* at 150. Otherwise, "virtually every case in which the United States successfully invokes the state secrets privilege would need to be dismissed." *Id.* Such an approach would constitute judicial abdication from the responsibility to decide cases on the basis of evidence "in favor of a system of conjecture." *Id.* And the

Supreme Court has cautioned against "precluding review of constitutional claims" and "broadly interpreting evidentiary privileges." *Id.* at 151 (first citing *Webster v. Doe*, 486 U.S. 592, 603-04 (1988), and then citing *United States v. Nixon*, 418 U.S. 683, 710 (1974)). "[A]llowing the mere prospect of a privilege defense," without more, "to thwart a citizen's efforts to vindicate his or her constitutional rights would run afoul" of those cautions. *Id.* Thus, where the government contends that dismissal is required because the state secrets privilege inhibits it from presenting a valid defense, the district court may properly dismiss the complaint only if it conducts an "appropriately tailored *in camera* review of the privileged record," *id.*, and determines that defendants have a legally meritorious defense that prevents recovery by the plaintiffs, *id.* at 149 & n.4.

CONCLUSION

The legal questions presented in this case have been many and difficult. We answer them on purely legal grounds, but of course realize that those legal answers will reverberate in the context of the larger ongoing national conversation about how reasonably to understand and respond to the threats posed by terrorism without fueling a climate of fear rooted in stereotypes and discrimination. In a previous case, we observed that the state secrets doctrine strikes a "difficult balance . . . between fundamental principles of our liberty, including justice, transparency, accountability and national security," and sometimes requires us to confront "an irreconcilable conflict" between those principles. *Jeppesen*, 614 F.3d at 1073. In holding, for the reasons stated, that the Government's assertion of the state secrets privilege does not warrant dismissal of this litigation in its en-

tirety, we, too, have recognized the need for balance, but also have heeded the conclusion at the heart of Congress's enactment of FISA: the fundamental principles of liberty include devising means of forwarding accountability while assuring national security.

Having carefully considered the Defendants' various arguments for dismissal other than the state secrets privilege, we conclude that some of Plaintiffs' search and religion allegations state a claim, while others do not. We therefore affirm in part and reverse in part the district court's orders, and remand for further proceedings in accordance with this opinion.

AFFIRMED in part, REVERSED in part, and REMANDED.

GOULD and BERZON, Circuit Judges, joined by WARDLAW, FLETCHER, and PAEZ, Circuit Judges, concurring in the denial of rehearing en banc:

Judge Bumatay's dissent from the denial of rehearing (the "dissent") is a veritable Russian doll of nestled mistakes and misleading statements—open one, and another stares back at you. The panel opinion itself belies most of the accusations. For brevity, we pay particular attention here to the dissent's most fundamental misperceptions of the panel's holdings.

I

At the core of this case lies a series of interwoven statutory interpretation issues surrounding the application of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801 *et seq*, in a civil action. The panel opinion concluded that a provision of that statute,

50 U.S.C. § 1806(f), supersedes the common law state secrets evidentiary privilege's limited dismissal remedy —not the protection of state secrets from disclosure— with regard to evidence or information related to electronic surveillance, and that the secrecy-protective procedures established by 50 U.S.C. § 1806(f), designed precisely for matters implicating national security concerns, apply to the plaintiffs' claims in this case against the government.

In concluding that § 1806(f)'s procedures apply, the panel opinion decidedly did *not*, as the dissent asserts, second guess the Executive's capacity to determine that certain evidence related to electronic surveillance is classified or touches on issues of national security, and therefore deserves protection from disclosure to litigants or the public. *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1081-82 (9th Cir. 2010) (en banc). Instead, the panel opinion resolved the discrete issue of what should happen in a civil case that involves such information: Need the case be dismissed, as it sometimes is to implement the common law state secrets privilege, or can it go forward but *without* disclosure of the information to the plaintiffs, under specially tailored litigation procedures that would in other contexts be impermissible as violative of the plaintiffs' rights as litigants?

Critically for present purposes, the classified material at issue is protected from disclosure under § 1806(f), just as it is under the state secrets privilege's dismissal option—it is just protected differently. To ensure that sensitive information is not inadvertently disclosed to the public, the § 1806(f) procedures require the district court to consider the material *ex parte* and *in camera*.

The government uses these very same procedures all the time when prosecuting suspected terrorists; the government does so by choice, and without any evident handwringing over whether the use of the § 1806(f) procedures might lead to the disclosure of state secrets. And the same *ex parte* and *in camera* review takes place when the state secrets privilege is invoked, to ascertain whether it is properly applicable and, if so, whether the case can go forward without the sensitive evidence or must be dismissed; that is exactly what happened in this case in the district court.[1]

II

The dissent's misleading assertions about the nature of the § 1806(f)'s procedures underpin its two major legal propositions, neither of which is rooted in the facts of this case, the text of FISA, or any binding precedent.

---

[1] The dissent notes § 1806(f) and (g)'s disclosure provisions, which are available only in exceptional circumstances. As far as we are aware, there has *never* been a disclosure under FISA. And, as the panel opinion noted: "As it is Plaintiffs who have invoked the FISA procedures, we proceed on the understanding that they are willing to accept those restrictions to the degree they are applicable as an alternative to dismissal, and so may not later seek to contest them." Amended Opinion at 49. In the unprecedented event that a district court *does* order disclosure, nothing in the panel opinion prevents the government from invoking the state secrets privilege's dismissal remedy as a backstop at that juncture. Finally, the panel does not, as the dissent asserts, "warn" district judges that failure to disclose evidence could constitute an abuse of discretion. Dissent at 134 n.9. The panel does not take any position on the appropriate standard of review for a district court's decision regarding the disclosure of FISA materials. Rather, we merely note the approach adopted in other circuits.

A

The dissent insists that the panel should have applied a "clear statement" rule to the question whether the § 1806(f) *ex parte*, *in camera* method of litigation displaces the state secrets evidentiary privilege's dismissal remedy.

The panel could not have applied a "clear statement" analysis. Our Circuit's binding precedent required the panel to ask whether FISA's § 1806(f)'s procedures "speak[] directly" to the question otherwise answered by the dismissal remedy in cases involving classified material related to electronic surveillance. *See Kasza v. Browner*, 133 F.3d 1159, 1167 (9th Cir. 1998) (internal quotation marks and emphasis omitted). As the panel opinion explained, the text, practice, purpose, and history of FISA and § 1806(f) all quite clearly demonstrate that the *ex parte* and *in camera* review established by § 1806(f) squarely answers the "speak directly" question.

The dissent maintains the "speaks directly" standard adopted in *Kasza* is wrong, because the state secrets evidentiary privilege has constitutional origins. *See* Dissent at 119, 129. The proposed new "clear statement" requirement—effectively, that Congress had to name the state secrets privilege, including its contingent dismissal remedy, to replace that remedy—is improper in the current context for two reasons.

First, no matter the origins or role of the state secrets privilege, at issue here is only the *dismissal remedy* that sometimes follows the successful invocation of the state secrets evidentiary privilege, when the case cannot as a practical matter be litigated without the privileged evidence. *Jeppesen Dataplan, Inc.*, 614 F.3d at 1082-83. "Ordinarily, simply excluding or otherwise

walling off the privileged information may suffice to protect the state secrets," but, "[i]n some instances . . . application of the privilege may require dismissal of the action." *Id.*

The dissent portrays the state secrets privilege as a magic wand that the Executive may wave to remove certain information from litigation or, if necessary, end the case. Not so. "The privilege belongs to the Government and must be asserted by it," but "[t]he court itself must determine whether the circumstances are appropriate for the claim of privilege." *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *see also El-Masri v. United States*, 479 F.3d 296, 312 (4th Cir. 2007). And the role of the court is especially pronounced when it must determine whether dismissal is necessary. *See Jeppesen Dataplan, Inc.*, 614 F.3d at 1082-83. So the dismissal remedy is not the state secrets privilege itself but a procedural exigency, sometimes imposed by the courts to prevent unfairness to the litigants once the evidentiary exclusion privilege is invoked and recognized with regard to certain evidence. Dismissal in the state secrets context is thus not grounded in separation of powers concerns.

Second, and more generally, as the panel opinion recounts, at heart the state secrets privilege is an *evidentiary* privilege, not a constitutional one. Amended Opinion at 58-59; *see In re United States*, 872 F.2d 472, 474-75 (D.C. Cir. 1989). *Reynolds*, which the dissent recognizes as the wellspring of "the modern state secrets doctrine," Dissent at 128, itself made this point:

> We have had broad propositions pressed upon us for decision. On behalf of the Government it has been urged that the executive department heads have power to withhold any documents in their custody

> from judicial view if they deem it to be in the public interest. Respondents have asserted that the executive's power to withhold documents was waived by the Tort Claims Act. Both positions have constitutional overtones which we find it unnecessary to pass upon, there being a narrower ground for decision.

345 U.S. at 6. As *General Dynamics Corp. v. United States*, 563 U.S. 478, 485 (2011), summarized, "*Reynolds* was about the admission of evidence. It decided a purely evidentiary dispute by applying evidentiary rules: The privileged information is excluded, and the trial goes on without it."

Or the trial doesn't go on, if the district court decides that dismissal is necessary. But in the narrow context of classified information related to electronic surveillance, FISA's procedures do away with the need for dismissal, by allowing the court to consider the relevant materials during the course of the litigation in the truncated and secrecy-protective manner established by § 1806(f).

B

The dissent also strives to insulate the government from suit by paring back the coverage of § 1806(f) and related provisions so as not to cover at all suits against the government. The dissent thus presents FISA, and specifically § 1806(f), as single-mindedly concerned with protecting the government's ability to prosecute criminal defendants without revealing national security secrets.

FISA is decidedly not so one-sided. The dissent never mentions a FISA provision, 50 U.S.C. § 1810, which authorizes affirmative actions against the government

challenging electronic surveillance material as unlawfully obtained. Ignoring § 1810, the dissent puts forward a view of the reach of § 1806(f)'s procedures much too narrow to accommodate the statute's provision for affirmative relief. Were the dissent's one-way-ratchet position correct, in a § 1810 affirmative suit, the need to consider the same evidence that was or should have been excluded in a prosecution of a defendant (because the surveillance used to collect the evidence is alleged to have been unlawful) could lead to dismissal of a § 1810 suit seeking damages for that same illegal surveillance.

To position these procedures as a one-way ratchet for the government, the dissent takes every opportunity to shrink the reach of § 1806(f) and related provisions to a scope much more circumscribed than their terms and purpose support. To highlight four of the dissent's efforts:

- To fit the dissent's narrative that § 1806(f) applies only when the government is on the offensive, the dissent maintains that the government does not intend to "use" the relevant information over which it has asserted the state secrets privilege—a requisite for the application of § 1806(f)'s procedures. But here, the government's primary reason for invoking the state secrets privilege's dismissal remedy *is* its asserted need to use classified information to defend itself if the case went forward. The government submitted, alongside the Attorney General's invocation of the state secrets privilege, an unclassified declaration stating that "[a]ddressing plaintiffs' allegations in this case will risk or require the disclosure of certain sensitive information con-

cerning counterterrorism investigative activity in Southern California, including in particular the nature and scope of Operation Flex."

- The dissent also takes the word "use" out of context. FISA's procedures apply "[w]henever the Government intends to enter into evidence or *otherwise use* or disclose in any trial, hearing, or other proceeding . . . any information obtained or derived from an electronic surveillance[.]" 50 U.S.C. § 1806(c) (emphasis added). In other words, the procedures apply whenever the government uses the information in "another way" or "any other way" than entering it into evidence. *See Otherwise*, The Oxford English Dictionary Online, https://www.oed.com/view/Entry/133247?redirectedFrom=otherwise#eid (last visited June 22, 2020).

- The dissent argues that, to trigger FISA's review procedures, "an aggrieved person" must be the defendant. Dissent at 138-139. But the statute is not unidirectional. The dissent takes the "against an aggrieved person" phrase out of context to suit the dissent's preferred ends. The statutory scheme establishes that § 1806(f)'s procedures apply "[w]henever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person." § 1806(c). A "trial, hearing, or other proceeding"

involves two parties, providing either an opportunity to introduce evidence—it is the *evidence* that is "against" someone.

- The dissent states that "§ 1806(f) authorizes the review of only a limited set of documents: the FISA 'application, order, and such other materials.'" Dissent at 132. But that is not what the statute says, and the full text of the relevant phrase tells an entirely different story: § 1806(f) authorizes the district court to review the "application, order, and *such other materials relating to the surveillance as may be necessary* to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." § 1806(f) (emphasis added). As used in the actual statute as opposed to the dissent's truncated version, "such" does not, as the dissent erroneously claims, refer only backwards to "application" and "order;" it also, and most prominently, applies forward to "materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." §?1806(f) [*sic*]; *see Such*, Merriam-Webster Online, https://www.merriam-webster.com/dictionary/such (last visited June 22, 2020) (defining "such" principally to mean "of a kind or character *to be* indicated or suggested") (emphasis added).

In conjunction with misreading the statute in these and other respects, the dissent avows that the panel opinion gives "unintended breadth" to FISA. Dissent at 142 (quoting *Yates v. United States*, 135 S. Ct. 1074, 1085 (2015)). But the only way to know what "breadth" is "in-

tended" is to read the statute. Section 1806(f) speaks in the broadest language possible. The procedures apply "*whenever* the Government intends to enter into evidence or otherwise use or disclose in *any* trial, hearing, or proceeding . . . *any* information obtained or derived from an electronic surveillance" or "*whenever any* motion or request is made . . . pursuant to *any other* statute or rule of the United States or *any* State before *any* court or *other* authority." (Emphases added). If that capacious language were not enough to maximize the provision's reach, every conceivable clause is separated by a disjunctive "or." Rather than "jam a square peg into a round hole," Dissent at 143, or "hide elephants in mouseholes," Dissent at 142 (quoting *Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001)), the panel opinion acknowledged that, when statutes use expansive language, we should understand that Congress did not mean for us to read in limitations that are not there.

* * *

The dissent is replete with quotations from Washington, Hamilton, and Jefferson, all making the indisputable point that, to protect our national interest, our government must be able to keep certain information secret. Neither the Founding Fathers' concerns about governmental secrecy nor broad issues of executive authority are at issue in this case. The question presented to the panel here was not whether the government should be able to keep classified material secret but how. The procedures established by § 1806(f) (which the government leans on heavily when it is the prosecutor) ensure secrecy. Under any reasonable reading of the statute, these procedures, when otherwise applicable, supersede the state secrets privilege's contingent dismis-

sal remedy and apply to the information at issue in this case.

For the forgoing reasons, we concur in the denial of rehearing en banc.

STEEH, Senior District Judge, statement regarding the denial of rehearing en banc:

Although, as a visiting judge sitting by designation, I am not permitted to vote on a petition for rehearing en banc, I agree with the views expressed by Judges Berzon and Gould in their concurrence in the denial of rehearing en banc.

BUMATAY, Circuit Judge, with whom CALLAHAN, IKUTA, BENNETT, R. NELSON, BADE, LEE, VANDYKE, Circuit Judges, join, and COLLINS and BRESS, Circuit Judges, join except for Section III.A.2, dissenting from the denial of rehearing en banc:

From the earliest days of our Nation's history, all three branches of government have recognized that the Executive has authority to prevent the disclosure of information that would jeopardize national security. Embodied in the state secrets privilege, such discretion lies at the core of the executive power and the President's authority as Commander in Chief. Indeed, these powers were vested in a single person precisely so that the Executive could act with the requisite "[d]ecision, activity, *secrecy*, and d[i]spatch." The Federalist No. 70 (Alexander Hamilton) (emphasis added).

In contrast to the broad constitutional design of the state secrets privilege, Congress passed the Foreign Intelligence Surveillance Act ("FISA") for a limited function—to establish procedures for the lawful electronic surveillance of foreign powers and their agents. Among other things, FISA provides a mechanism for in camera, ex parte judicial review of electronic surveillance evidence when the government tries to use such evidence, or a surveilled party tries to suppress it. *See* 50 U.S.C. § 1806(f).[1]

By its plain text and context, § 1806(f) provides procedures to determine the *admissibility* of electronic surveillance evidence—a commonplace gatekeeping function exercised by courts throughout this country. When the provision is triggered, courts review only a limited set of documents, the FISA application, order, and like materials, and may generally only suppress the evidence if it was unlawfully obtained. § 1806(f), (g). Thus, § 1806(f) coexists with the state secrets privilege by providing judicial oversight over the government's affirmative use of electronic surveillance evidence, while preserving the Executive's constitutional prerogative to protect national security information.

But today, the Ninth Circuit, once again, strains the meaning of a statute and adopts a virtually boundless

---

[1] All statutory references are to Title 50 of the United States Code. In relevant part, § 1806(f) provides, when triggered, "the United States district court . . . shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted."

view of § 1806(f). Under the court's reading, this narrow provision authorizes judicial review of any evidence, on any claim, for any purpose, as long as the party's allegations relate to electronic surveillance. With this untenably broad interpretation, the court then rules that the judicial branch will not recognize the state secrets privilege over evidence with any connection to electronic surveillance. Most alarming, this decision may lead to the disclosure of state secrets to the very subjects of the foreign-intelligence surveillance. With this, I cannot agree.

Our court's decision ignores that Congress articulated no directive in FISA to displace the state secrets privilege—even under the most generous abrogation standards. More fundamentally, the court should have ensured that Congress was unmistakably clear before vitiating a core constitutional privilege. When the Supreme Court confronts a legislative enactment implicating constitutional concerns—federalism or separation of powers—it has commonly required a clear statement from Congress before plowing ahead. It has done so out of a due respect for those constitutional concerns. The state secrets privilege deserves the same respect.

In discovering abrogation of the state secrets privilege more than 40 years after FISA's enactment, our court disrupts the balance of powers among Congress, the Executive, and the Judiciary. We have previously recognized that the state secrets doctrine preserves the difficult balance among "fundamental principles of our liberty, including justice, transparency, accountability and national security." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1073 (9th Cir. 2010) (en banc). Our refusal to reexamine this case now tips that balance

in favor of inventive litigants and overzealous courts, to the detriment of national security. Moving forward, litigants can dodge the state secrets privilege simply by invoking "electronic surveillance" somewhere within the Ninth Circuit. And in defending such cases, the government may be powerless to prevent the disclosure of state secrets. For this reason, I respectfully dissent from the denial of rehearing en banc.

I.

In this case, Yassir Fazaga and his co-plaintiffs sued the United States, the FBI, and FBI special agents, for using an informant to gather information from the Muslim community in Southern California. Their complaint asserted numerous constitutional and statutory causes of action alleging unlawful searches and surveillance and violations of their religious liberty.

Soon after the suit was filed, the FBI asserted the state secrets privilege over information related to its investigation. Through a declaration of the Attorney General, the government warned that proceeding on the claims risked the disclosure of state secrets.[2] Accordingly, the government moved to dismiss the religious liberty claims.

After scrutinizing the government's classified and unclassified declarations, the district court validated its assertion of the privilege. The court found that the litigation involved intelligence that, if disclosed, would sig-

---

[2] Specifically, the government sought to withhold evidence that would (1) confirm or deny the particular targets of the investigation; (2) reveal the initial reasons for opening the investigation, the materials uncovered, or the status and results of the investigation; and (3) reveal particular sources or methods used.

nificantly compromise national security. Because the risk of disclosure could not be averted through protective orders or other restrictions, the court dismissed all but one of the claims.

On appeal, a panel of this court reversed. The panel first held that FISA abrogated the state secrets privilege. It thought that § 1806(f) "speaks directly" to the same concerns as the state secrets privilege and, thus, displaced it—despite recognizing that the privilege "may" have a "constitutional core" or "constitutional overtones." Am. Op. at 58-59. Next, the court held that § 1806(f)'s review procedures were triggered in this case. As a result, the court instructed the district court to use those procedures to review *any* evidence relating to the alleged electronic surveillance—even the evidence that the government asserted constituted state secrets.

Because each of these holdings is erroneous, we should have reviewed this case en banc.

II.

Abrogation of ordinary common law is rooted in due respect for Congress. "Federal courts, unlike state courts, are not general common-law courts and do not possess a general power to develop and apply their own rules of decision." *City of Milwaukee v. Illinois*, 451 U.S. 304, 312 (1981). Accordingly, once "the field has been made the subject of comprehensive legislation," federal common law must yield to the legislative enactment. *Id.* at 314. In the ordinary case, Congress need not affirmatively proscribe the use of federal common law, but it must "speak directly" to the questions previously addressed by common law. *Id.* at 315.

Yet this is no ordinary case. Here, the court didn't abrogate run-of-the-mill, judicially created common law —it displaced an executive privilege. And it did so while summarily dismissing the constitutional and separation-of-powers implications of its holding. Before supplanting a privilege held by a co-equal branch of government, courts would be wise to consider the Constitution and the history of the privilege at issue. As Justice Scalia recognized, "a governmental practice [that] has been open, widespread, and unchallenged since the early days of the Republic" deserves special deference. *NLRB v. Noel Canning*, 573 U.S. 513, 572 (2014) (Scalia, J., concurring) (citations omitted). This approach should guide our analysis here.

A.

Article II of the Constitution commands that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. And the President is also designated as the "Commander in Chief of the Army and Navy of the United States." U.S. Const. art. II, § 2.

By these terms, the Constitution was originally understood to vest the President with broad authority to protect our national security. *See Hamdi v. Rumsfeld*, 542 U.S. 507, 580 (2004) (Thomas, J., dissenting) ("The Founders intended that the President have primary responsibility—along with the necessary power—to protect the national security and to conduct the Nation's foreign relations."). As Hamilton observed, a single Executive could better act with "[d]ecision, activity, secrecy, and d[i]spatch" as would be required to respond to the national security crises of the day. The Federalist No. 70 (Alexander Hamilton).

Secrecy, at least at times, is a necessary concomitant of the executive power and command of the Nation's military. As commander of the Continental Army, George Washington explained to Patrick Henry that "naturally . . . there are some Secrets, on the keeping of which so, depends, oftentimes, the salvation of an Army: Secrets which cannot, at least ought not to, be [e]ntrusted to paper; nay, which none but the Commander in Chief at the time, should be acquainted with."[3]

Given the Executive's inherent need for secrecy, it comes as no surprise that early presidents regularly asserted a privilege over the disclosure of sensitive information.[4] In 1792, when President Washington found himself faced with the first-ever congressional request for presidential materials, he recognized an executive privilege to avoid disclosure of secret material. *See* Abraham D. Sofaer, *Executive Power and the Control of Information: Practice Under the Framers*, 1977 Duke L.J. 1, 5-6. Washington's Cabinet, including Hamilton and Jefferson, agreed "that the executive ought to communicate such papers as the public good would permit, and ought to refuse those, the disclosure of which would

---

[3] Letter from George Washington to Patrick Henry (Feb. 24, 1777), Library of Congress, https://www.loc.gov/resource/mgw3h.001/?sp=26&st=text.

[4] Although this history recounts executive privileges in general, the state secrets privilege has been described as a "branch of the executive privilege." *Marriott Int'l Resorts, L.P. v. United States*, 437 F.3d 1302, 1307 (Fed. Cir. 2006). To the extent there are distinctions among executive privileges, the state secrets privilege is more inviolable. *See United States v. Nixon*, 418 U.S. 683, 706 (1974) (distinguishing between privileges based "solely on the broad, undifferentiated claim of public interest in the confidentiality of such conversations" with those asserted from the "need to protect military, diplomatic, or sensitive national security secrets").

injure the public." *Id.* at 6 (quoting The Complete Jefferson 1222 (S. Padover ed. 1943)); *see also* Mark J. Rozell, *Restoring Balance to the Debate over Executive Privilege: A Response to Berger*, 8 Wm. & Mary Bill Rts. J. 541, 556 (2000).

President Jefferson, even as a prominent critic of an overly strong executive branch, held the same view on the need for secrecy. As he put it in 1807, "[a]ll nations have found it necessary, that for the advantageous conduct of their affairs, some of these proceedings, at least, should remain known to their executive functionary only. He, of course, from the nature of the case, must be the sole judge of which of them the public interests will permit publication."[5] Similarly, Jefferson wrote to the prosecutor of the Aaron Burr case to explain that it was "the necessary right of the President . . . to decide, independently of all other authority, what papers, coming to him as President, the public interests permit to be communicated, & to whom."[6]

Founding-era Presidents were not alone in their view. Members of Congress also respected some degree of executive privilege. When Washington refused a congressional request for materials, then-Representative James Madison disagreed with Washington's refusal, but also recognized that "the Executive had a right, under a due responsibility, also, to withhold information, when of a nature that did not permit a disclosure of it at

---

[5] Letter from Thomas Jefferson to George Hay (June 17, 1807), Library of Congress, https://www.loc.gov/resource/mtj1.038_0446_0446/?st=text.

[6] Letter from Thomas Jefferson to George Hay (June 12, 1807), Library of Congress, https://www.loc.gov/resource/mtj1.038_0446_0446/?st=text.

the time." 5 Annals of Cong. 773 (1796); Sofaer, *supra* at 12. Others went further, asserting, for example, that the President "had an undoubted Constitutional right, and it would be his duty to exercise his discretion on this subject, and withhold any papers, the disclosure of which would, in his judgment, be injurious to the United States." 5 Annals of Cong. 675 (1796) (remarks of Rep. Hillhouse).

Congress's early actions also reflected a deference to the Executive's authority to limit disclosures. When seeking information from the President, Congress narrowed its requests to such presidential papers "of a public nature," 3 Annals of Cong. 536 (1792), or "as he may think proper," 4 Annals of Cong. 250-51 (1794), and excluded "such [papers] as he may deem the public welfare to require not to be disclosed." 16 Annals of Cong. 336 (1807). Thus, early Congresses "practically always" qualified their requests for foreign-affairs information to those documents that "in [the President's] judgment [were] not incompatible with the public interest." Henry M. Wriston, *Executive Agents in American Foreign Relations* 121-22 (1929).

Like the Executive and Congress, the Judiciary has long recognized an executive privilege over sensitive information. Chief Justice Marshall suggested that if the Attorney General "thought that any thing was communicated to him in confidence he was not bound to disclose it" in the litigation. *Marbury v. Madison*, 5 U.S. 137, 144 (1803); *see also* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 Geo. Wash. L. Rev. 1249, 1271 (2007). And in response to President Jefferson's objection to producing a letter in the Burr trial, Chief Justice Marshall explained that

there was "nothing before the court which shows that the letter in question contains any matter the disclosure of which would endanger the public safety," but "[t]hat there may be matter, the production of which the court would not require, is certain." *United States v. Burr*, 25 F. Cas. 30, 37 (C.C.D. Va. 1807); *see also* Chesney, *supra* at 1272-73 (arguing that the Burr trial is significant for Marshall's introduction of the idea that "risk to public safety might impact discoverability of information held by the government"). Perhaps anticipating the modern-day state secrets privilege, Marshall made clear "that the remedy he contemplated for executive withholding would be dismissal of the prosecution, rather than an order directing the President to appear or punishing any executive officer." Sofaer, *supra* at 17.

The Supreme Court also recognized that President Lincoln "was undoubtedly authorized during the war, as commander-in-chief of the armies of the United States, to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy[.]" *Totten v. United States*, 92 U.S. 105, 106 (1875). In *Totten*, the Court dismissed a contract claim where the very existence of the alleged contract needed to be concealed. *Id.* Such concealment was a reality "in all secret employments of the government in time of war, or upon matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our government in its public duties, or endanger the person or injure the character of the agent." *Id.*

Consistent with early historical practice and Founding-era understandings, modern courts have recognized the Article II dimension of executive privileges. *See Nixon*,

418 U.S. at 711 (explaining that when a privilege against disclosure relates to the "effective discharge of a President's powers, it is constitutionally based"); *Franchise Tax Bd. of California v. Hyatt*, 139 S. Ct. 1485, 1498-99 (2019) (identifying the "executive privilege" as one of the "constitutional doctrines" that are "implicit in the [Constitution's] structure and supported by historical practice"); *see also Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988) ("The authority to protect [national-security] information falls on the President as head of the Executive Branch and as Commander in Chief.").[7] As Justice Jackson succinctly put it: "The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are nor ought to be published to the world." *Chicago & S. Air Lines v. Waterman S. S. Corp.*, 333 U.S. 103, 111 (1948).

This brings us to the modern state secrets doctrine, articulated in *United States v. Reynolds*, 345 U.S. 1 (1953). In *Reynolds*, the Court recognized the Executive's "well established" privilege against revealing military and state secrets. *Id.* at 7-8. The Court held that "even the most compelling necessity cannot overcome the claim of privilege" if state secrets are at stake. *Id.* at 11; *see also El-Masri v. United States*, 479 F.3d 296, 303 (4th Cir. 2007) ("Although the state secrets privilege was developed at common law, it performs a function of constitutional significance, because it allows the execu-

[7] None of this is to say that the Executive has an absolute privilege to prevent the disclosure of material under any circumstance. I explore this history only insofar as it bears on the particular issue in this case—the proper standard to apply before abrogating the state secrets privilege.

tive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities."). As an en banc court, we've respected the ability of the government to seek to "completely remove[]" state secrets from litigation or even seek "dismissal of the action." *Jeppesen*, 614 F.3d at 1082-83. And in evaluating the assertion of the privilege, we "defer to the Executive on matters of foreign policy and national security." *Id.*

B.

Given this constitutional and historical background, courts ought to tread carefully before jettisoning the state secrets privilege. Here, we should have done so by requiring a clear congressional statement before displacing the privilege. By waiting for a clear statement, we would have avoided assuming that Congress has "by broad or general language, legislate[d] on a sensitive topic inadvertently or without due deliberation." *Spector v. Norwegian Cruise Line Ltd.*, 545 U.S. 119, 139 (2005) (plurality opinion). Instead, the court today undermines a longstanding executive privilege by finding abrogation lurking in FISA's murky text.

Unlike abrogation of ordinary common law, which shows our deference to Congress, the displacement of the state secrets privilege creates a tension between Congress and the Executive because we elevate a statute over a constitutionally based privilege. As the Court advises, we should be "reluctant to intrude upon the authority of the Executive in military and national security affairs" until "Congress specifically has provided otherwise." *Egan*, 484 U.S. at 530. Thus, whether FISA merely "speaks directly" to the same concerns as the privilege should not be sufficient to deprive the Execu-

tive of a constitutionally derived right. Instead, we should have constrained ourselves to respecting the privilege unless and until a statute unmistakably and unquestionably dictates otherwise.

This is not a novel idea. When a matter implicates constitutional concerns, the Court has regularly required a clear statement. *See, e.g.*, *Will v. Michigan Dep't of State Police*, 491 U.S. 58, 65 (1989) (requiring Congress to be "unmistakably clear" before altering the "usual constitutional balance between the States and the Federal Government"); *Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992) (requiring an express statement before subjecting presidential action to APA review "[o]ut of respect for the separation of powers and the unique constitutional position of the President"). The Court has likewise required a clear statement before abrogating Indian treaty rights, out of a respect for tribal sovereignty. *See United States v. Dion*, 476 U.S. 734, 739 (1986) (explaining the reluctance to find abrogation absent "explicit statutory language").

Applying such a standard is also consistent with the constitutional-avoidance canon. *See United States ex rel. Attorney Gen. v. Delaware & Hudson Co.*, 213 U.S. 366, 408 (1909) ("[W]here a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, our duty is to adopt the latter."). Thus, when "a particular interpretation of a statute invokes the outer limits of Congress' power," as is the case here, we should "expect a clear indication that Congress intended that result." *I.N.S. v. St. Cyr*, 533 U.S. 289, 299 (2001).

All in all, we should be "loath to conclude that Congress intended to press ahead into dangerous constitutional thickets in the absence of firm evidence that it courted those perils." *Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 466 (1989). But the court here is undeterred. It reads FISA as abrogating the privilege despite the lack of any firm evidence that Congress sought to do so. And rather than consulting the Constitution or the history of the state secrets privilege, the court simply waves off the privilege as something that "may" have a "constitutional core" or "constitutional overtones." Am. Op. at 58-59. Respectfully, when we suspect that an executive privilege "may" have a "constitutional core," we should do more before tossing it aside. Had we done so here, perhaps we would've recognized that the Article II roots of the privilege and its long history require that Congress be unmistakably clear before we simply replace it with a congressional enactment. And because FISA makes *no* mention of the state secrets privilege, the statute would fall pitifully short of this standard.

C.

Even if we should stick with the run-of-the-mill, "speaks directly" standard for displacement, FISA still falls short. Demonstrating that a statute speaks directly to the same questions as the common law is no low bar. *See, e.g.*, *United States v. Texas*, 507 U.S. 529, 535 (1993) (holding that silence in a statute "falls far short of an expression of legislative intent to supplant the existing common law in that area"). The court's analysis does not clear this bar.

At the outset, the court's opinion critically fails to recognize the circumscribed purpose of § 1806(f)—to

provide a mechanism to review the admissibility of electronic surveillance evidence. *See infra* section III. Determining the admissibility of evidence is an everyday function of courts. Section 1806(f) merely adds extra precautions in the case of electronic surveillance evidence. Nothing more. The statute's design is in stark contrast to the constitutional purpose of the state secrets privilege—to ensure our "defer[ence] to the Executive on matters of foreign policy and national security" and to prevent courts from "second guessing the Executive in this arena." *Jeppesen*, 614 F.3d at 1081-82. Contrary to the court's interpretation, § 1806(f) and the state secrets privilege stand side by side, maintaining the Judiciary's control over the admissibility of evidence on one hand while deferring to the Executive's authority to protect national security information on the other.

Relatedly, the court also overlooks a significant limitation on § 1806(f)'s scope of review. Section 1806(f) authorizes the review of only a limited set of documents: the FISA "application, order, and such other materials." The court's decision treats this language as allowing review of "any" materials tangentially related to electronic surveillance. Am. Op. at 102-103. But the phrase "such other materials" cannot be read so boundlessly. *See Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 114-15 (2001) ("[W]here general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words."). Even without this canon, ordinary users of the English language understand the word "such" to mean "something similar," "of the same class, type, or sort," or "of the character, quality, or extent previously indicated or

implied." *Such*, Webster's Ninth New Collegiate Dictionary (1986).[8]

Thus, the phrase "such other material" refers to documentary evidence like the "application" and "order"; in other words, materials containing information necessary to authorize the surveillance. *See, e.g.*, § 1804(c) ("The judge may require the applicant to furnish *such other information* as may be necessary to make the determinations required [to authorize the surveillance under § 1804].") (emphasis added). It does not broadly reach *any* evidence related to electronic surveillance as the court's decision assumes. It certainly does not reach the evidence over which the government asserted the privilege—which goes far beyond FISA documents. *See supra* note 2.

Furthermore, § 1806(f) didn't create anything novel to suggest displacement of the state secrets privilege. The court's opinion treats § 1806(f) as enacting "an alternative mechanism" of ex parte, in camera review, which shows Congress's intent to "eliminate[] the need to dismiss the case entirely" under the state secrets privilege. Am. Op. at 61-62. Not so. Pre-FISA courts already conducted in camera and ex parte review with regularity. *See United States v. Belfield*, 692 F.2d 141, 149 (D.C. Cir. 1982) (recognizing that prior to FISA courts had "constantly" and "uniformly" held that "the legality of electronic, foreign intelligence surveillance may, even should, be determined on an in camera, ex

---

[8] Continuing to ignore this longstanding canon of interpretation, the concurrence to the denial of rehearing en banc doubles down on a boundless reading of this phrase. But this reading treats the word "such" as if it meant "any." We should apply the statute as Congress wrote it, not as we might wish it to be.

parte basis"). Given that ex parte, in camera review procedures coexisted with the state secrets privilege before FISA, there's no reason to construe Congress's codification of such procedures as an intent to eliminate the privilege.

Nor does § 1806(f)'s triggering process—the filing of an affidavit under oath by the Attorney General—support abrogation. The court views the superficial similarity between the assertion of the state secrets privilege by the head of a department, *see Jeppesen*, 614 F.3d at 1080, and § 1806(f)'s affidavit requirement as evidence that Congress intended abrogation. Such evidence actually cuts the other way. Under FISA, the definition of "Attorney General" permits a number of lower-ranked Department of Justice officials to invoke FISA's judicial review procedures, *see* § 1801(g), which makes sense given its main use in criminal prosecutions. By contrast, the head of *any* department has the *non-delegable* authority to assert the state secrets privilege. *Jeppesen*, 614 F.3d at 1080. Nothing in FISA's text suggests that Congress sought to remove the privilege from the hands of the Secretary of State, the Director of National Intelligence, and other cabinet heads, and simply transfer it to the Attorney General and his subordinates. Contrary to the court's assessment, the difference between who can assert the privilege and who can invoke § 1806(f) reaffirms that FISA coexists with, rather than displaces, the state secrets privilege.

Finally, the court's view of FISA as a replacement for the state secrets privilege ignores that the provision not only authorizes but *mandates* disclosure. *See* § 1806(g) (requiring the court to disclose evidence "to the extent that due process requires discovery or disclosure"); *see*

also § 1806(f) (authorizing the court to disclose evidence to the aggrieved person when "necessary to make an accurate determination of the legality of the surveillance"). And under the court's broad reading, FISA may very well authorize disclosure of state secrets to the very subjects of the surveillance. *See* Am. Op. 68 (holding that plaintiffs' request for electronic surveillance evidence triggers § 1806(f) review).[9]

But the state secrets privilege does not tolerate *any* disclosure—not even in camera and ex parte—if it can be avoided. *See Reynolds*, 345 U.S. at 10 ("[T]he court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers."). Such disclosures, when involving national security secrets,

---

[9] For the first time, Judge Berzon announces that the panel's opinion is actually limited to the state secrets privilege's dismissal remedy and that the government is free to reassert the privilege if the district court orders disclosure. *See* Concurrence at 110 n.1. This is news to anyone reading the panel opinion, which explicitly authorizes the district court to "disclose" state secrets evidence to the "plaintiffs." *See* Am. Op. at 103. The opinion goes so far to warn that "*not*" disclosing such evidence could constitute an abuse of discretion. *Id.* at 103 n.49 (emphasis added).

Nevertheless, that the panel needs to amend its opinion through a nonbinding concurrence is reason enough for us to have reheard this case en banc. We owe the district courts and litigants a clear statement of the law—especially in a case implicating national security concerns. More fundamentally, this newly crafted limitation of the court's holding doesn't alter any of the concerns raised in this dissent and in many ways exacerbates them. The court's holding, even as purportedly limited, impinges on a constitutionally based privilege based on a misreading of FISA. And if raising concerns about the court's degradation of separation of powers and our constitutional design makes me a "veritable Russian doll" maker, *see* Concurrence at 108, then bring on the dolls.

are inimical to the secrecy afforded to the Executive under Article II. Thus, FISA fails to speak directly to the paramount concern for the secrecy at the heart of the state secrets privilege.

Given the silence of the statutory text, it's unsurprising that the court's opinion resorts to legislative history to support abrogation. But "legislative history is not the law." *Epic Sys. Corp. v. Lewis*, 138 S. Ct. 1612, 1631 (2018). We "have no authority to enforce a principle gleaned solely from legislative history that has no statutory reference point." *Shannon v. United States*, 512 U.S. 573, 584 (1994) (cleaned up). Even so, from hundreds of pages of legislative history, the court excavates only vague quotes describing FISA as a "fundamental reform" aimed at curbing unchecked executive surveillance. *See* Am. Op. at 63-64. The court can't even muster up a single floor statement mentioning the state secrets privilege. Even for those who would rely on legislative history, this alone should end the inquiry.

Nevertheless, the legislative history shows that—contrary to the court's view—the state secrets privilege coexists with FISA. For example, a committee report notes that preexisting "defenses against disclosure," which would include the state secrets privilege, were intended to be undisturbed by FISA. *See* H.R. Rep. No. 95-1283, at 93 (1978). Another report explained that even when § 1806(f) applied, the government could still "prevent[]" the court's "adjudication of legality" simply by "forgo[ing] the use of the surveillance-based evidence" where disclosure of such evidence "would damage the national security." S. Rep. No. 95-701, at 65 (1978). And another explains that § 1806(f) was crafted "to prevent these carefully drawn procedures from be-

ing bypassed by the inventive litigant." H.R. Rep. No. 95-1283, at 91.

Ultimately, despite the lengthy excursion into FISA's legislative history, the court simply ignores material that undermines its interpretation. We're instead offered only generic, cherry-picked quotes about FISA — proving yet again that relying on legislative history is "an exercise in looking over a crowd and picking out your friends." *Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 568 (2005) (cleaned up). But if § 1806(f) was not meant for "inventive litigants," it was equally not meant for inventive courts.

III.

Most frustrating about our court's decision here is that § 1806(f) *doesn't even apply* to plaintiffs' case. Section 1806(f) isn't a freestanding vehicle to litigate the merits of any case involving electronic surveillance. FISA's review procedures are triggered only to determine the admissibility of the government's electronic surveillance evidence. In this case, the government never sought to admit and plaintiffs never sought to suppress any such evidence. Accordingly, § 1806(f) wasn't invoked. Yet the court creatively interprets two clauses of the statute to foist FISA's review mechanism into this case. We should have corrected this misinterpretation through en banc review.

A.

Section 1806(f)'s review procedures are triggered if the government gives notice that it "intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding . . . , against an aggrieved person, any information obtained or derived from

an electronic surveillance of that aggrieved person[.]" § 1806(c), (f). The court held that when the government asserted the state secrets privilege it effectively gave notice that it intended to "use" the evidence against plaintiffs. This is wrong for two separate reasons.

1.

First, § 1806(c) doesn't apply because the government isn't seeking to *use* the state secrets as evidence. By asserting the privilege, the government is not *using* evidence in any reasonable sense of the word. Quite the opposite: the government seeks to remove this evidence to avoid disclosing state secrets. *See Jeppesen*, 614 F.3d at 1079 ("A successful assertion of privilege under *Reynolds* will remove the privileged evidence from the litigation."). The court suggests that it "is precisely because the Government would like to use this information to defend itself that it has asserted the state secrets privilege." Am. Op. at 67. But this is precisely backwards. It transforms the government's expressed *inability to use* evidence into an expressed intent to use it. Such upside-down logic should not stand.

And no matter what tortured conception of "use" the court conjures up here, to "use" something means to do so for its intended purpose. *Smith v. United States*, 508 U.S. 223, 242 (1993) (Scalia, J., dissenting). "When someone asks, 'Do you use a cane?,' he is not inquiring whether you have your grandfather's silver-handled walking stick on display in the hall; he wants to know whether you *walk* with a cane." *Id.* So too here: the government is not "using" the evidence merely by asserting the privilege over it. Evidence is "used" when it is being offered for admission or disclosed for some other evidentiary purpose.

2.

Second, it's doubtful that § 1806(c) could apply here since there was no proceeding against "an aggrieved person." By its terms, this provision applies only to a "trial, hearing, or other proceeding" "against an aggrieved person." § 1806(c). This interpretation flows from the nearest-reasonable-referent canon. *See* Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation of Legal Texts 140-41 (2012) ("When the syntax involves something other than a parallel series of nouns or verbs, a prepositive or postpositive modifier normally applies only to the nearest reasonable referent."). It's also consistent with ordinary usage. Although the court now proclaims the opposite, *see* Am. Op. at 70, we commonly refer to trials, hearings, and proceedings as being "against" a party.[10] Instead, the court curiously views "against an aggrieved person" as modifying the phrase "information obtained or derived." But under that odd interpretation, this phrase would be modified *twice* by "aggrieved person." The statute would be triggered by the government's use of "any information obtained or derived [against the aggrieved person] from an electronic surveillance of that aggrieved person." § 1806(c). That is not a sensical reading.[11]

---

[10] *See, e.g., Paine v. City of Lompoc*, 265 F.3d 975, 986 (9th Cir. 2001) ("trial against these two defendants"); *United States v. Branch*, 368 F. App'x 842, 844 (9th Cir. 2010) ("misconduct hearing against the government"); *Lopez-Aguilar v. Barr*, 948 F.3d 1143, 1146 (9th Cir. 2020) ("removal proceedings against Lopez-Aguilar").

[11] The phrase "against an aggrieved person" also doesn't modify "enter into evidence or otherwise use or disclose." For adherents to the familiar surplusage canon, this reading would render the phrase completely superfluous. After all, who else is the government going to use the evidence against but the aggrieved person? Additionally, in

B.

Perhaps sensing the weakness of its § 1806(c) reasoning, the court serves an alternative explanation for how FISA's review procedures were triggered. Section 1806(f) also provides that its procedures are invoked:

> whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter[.]

§ 1806(f).

By its context, this clause is designed to funnel an aggrieved person's evidentiary motions and requests—which could be brought under a myriad of preexisting statutes or rules—into § 1806(f)'s admissibility review procedures. It is not an independent grant of authority to force government disclosure under § 1806(f) anytime, for any reason, for any evidence, as long as a party has some claim relating to electronic surveillance.

But the court holds that the clause was triggered because the plaintiffs' complaint requested injunctive re-

---

ordinary English, we don't often speak about "disclos[ing]" information "against" someone. And if this construction was intended, we would have expected Congress to make this point clear by placing the phrase closer to the verbs it modifies. *See United States v. Nader*, 542 F.3d 713, 717-18 (9th Cir. 2008) ("A prepositional phrase with an adverbial or adjectival function should be as close as possible to the word it modifies to avoid awkwardness, ambiguity, or unintended meanings.") (quoting The Chicago Manual of Style ¶ 5.167 (15th ed. 2003)).

lief ordering the government to destroy or return any unlawfully obtained materials. According to the court, by asking for the "return" of electronic surveillance, the complaint's *prayer for relief* serves as a "request[]" to "obtain" that information within the meaning of § 1806(f). Am. Op. 68.

Contrary to the court's expansive interpretation, this clause is limited to procedural motions pertaining to the admissibility of evidence, like the familiar "motion[s]" to "discover, obtain, or suppress." § 1806(f). The clause's use of the word "request" does not change this analysis since it must be read alike with "motion." *See Freeman v. Quicken Loans, Inc.*, 566 U.S. 624, 634-35 (2012) (applying the "commonsense canon" that "a word is given more precise content by the neighboring words with which it is associated"). In this context, these two terms refer to procedural actions such as a "production request" or a "motion to discover evidence," not substantive requests for relief.[12]

We're also not to read "motion or request" in a vacuum. The provision refers to motions and requests "[made] pursuant to any other statute or rule . . . to discover, obtain, or suppress evidence or information." § 1806(f). This context makes clear that that the provision covers only procedural motions or requests, not plaintiffs' substantive claims for relief. It likewise con-

---

[12] Seemingly whenever the phrase "motion or request" appears it refers to a procedural action. *See, e.g.*, 17 U.S.C. § 803(b)(6)(C)(v) ("motion or request to compel production"); Fed. R. Crim. P. 29, Advisory Comm. Notes to 2005 amendments ("motion or request" for an extension of time); Charles A. Wright et al., Federal Practice and Procedure: Criminal § 261 (4th ed. 2020 Update) (Rule 12(c) authorizes time for "making of pre-trial motions or requests").

firms that the clause is not an independent grant of authority, but relies on other statutes and rules—which would remain subject to evidentiary privileges.

In treating plaintiffs' complaint as a request sufficient to trigger § 1806(f), the court reads too much into the word "obtain," which must be read in the context of "the company it keeps." *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995). Here, "obtain" is spliced between "discover" and "suppress," both of which are procedural, evidentiary actions having nothing to do with substantive claims or injunctive relief. Accordingly, "obtain" is similarly limited to pretrial actions aimed at evaluating the admissibility of evidence. *See, e.g.*, Fed. R. Civ. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case[.]").

FISA's structure also confirms the clause's limitation to pretrial motions relating to the admissibility of evidence. All of the other triggering mechanisms of § 1806(f)—subsections (c), (d), and (e)—are pretrial, procedural actions to secure a ruling on the admissibility of evidence. This clause must be read in a similar light to avoid "giving unintended breadth to the Acts of Congress." *Yates v. United States*, 135 S. Ct. 1074, 1085 (2015). It would be odd for Congress to ambiguously bury a substantive right for plaintiffs to "obtain" national security secrets in the muddled language of § 1806(f). We know that this can't be the case because Congress does not "hide elephants in mouseholes." *Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001).

Additionally, FISA does not recognize injunctive relief. *ACLU Found. of S. California v. Barr*, 952 F.2d 457, 470 (D.C. Cir. 1991) ("Not only does § 1806(f) not create or recognize a cause of action for an injunction or for a declaratory judgment, but the scheme it sets up makes clear that nothing in FISA can be read to create such a cause of action."). It can't be the case that § 1806(f) is triggered by a request for substantive relief that FISA itself does not contemplate.[13]

Finally, this clause must be read in context of FISA's single remedy after § 1806(f) review—the "suppress[ion of] the evidence" or "*otherwise* grant[ing] the motion of the aggrieved person." § 1806(g) (emphasis added). Thus, these motions and requests, however styled, all lead down the same road—suppression of evidence, or relief in aid of that remedy. *Cf. James v. United States*, 550 U.S. 192, 218 (2007) (Scalia, J., dissenting) (recognizing that "'otherwise' is defined as '[i]n a different manner' or 'in another way,'" so the use of the word signals other ways of doing something of the same *character* as what preceded it). As the heading of this provision confirms, the district court's review can result in either "[s]uppression of evidence" or "denial of motion." § 1806(g) (heading). Thus, whether they're to "discover,

---

[13] The concurrence makes much ado over § 1810, which authorizes a cause of action for FISA violations. But the fact that the privilege "could" lead to a dismissal of a § 1810 suit, Concurrence at 113-114, is largely irrelevant. The same is true of any other cause of action. And just because claims *could* be dismissed after a valid privilege assertion doesn't mean all of them will be. Look no further than *this very case*: the government did not move to dismiss Plaintiffs' § 1810 claim based on the privilege and the claim is going forward (and would've gone forward even without the panel's abrogation of the privilege).

obtain, or suppress," these motions and requests only relate to the ultimate determination of the admissibility of evidence. Here, plaintiffs have neither a "motion to suppress," nor any other motion to "otherwise grant," should the district court rule in their favor after the § 1806(f) review. Accordingly, try as it might, the court can't jam a square peg into a round hole. Section 1806(f) doesn't apply here.

IV.

The court's decision today seriously degrades the Executive's ability to protect our Nation's secrets and I fear it is only a stepping stone to further erosions. By abrogating the state secrets privilege, we not only upset the balance of power among co-equal branches of government, but we also do damage to a right inherent in the constitutional design and acknowledged since our Nation's founding. And we do so without clear evidence that this is the result Congress sought. For these reasons, I respectfully dissent from the denial of rehearing en banc.

APPENDIX C

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

Case No. 8:11-cv-00301-CJC(VBKx)

YASSIR FAZAGA, ALI UDDIN MALIK,
YASSER ABDELRAHIM, PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL.,
DEFENDANTS

Aug. 14, 2012

ORDER GRANTING DEFENDANTS' MOTIONS TO DISMISS BASED ON THE STATE SECRETS PRIVILEGE

CORMAC J. CARNEY, District Judge.

I. INTRODUCTION

The present case involves a group of counterterrorism investigations by the Federal Bureau of Investigation ("FBI"), dubbed "Operation Flex," in which the FBI engaged a covert informant to help gather information on certain, unidentified individuals from 2006 to 2007. Although some of the general facts about Operation Flex, including the identity of one informant, Craig Monteilh, have been disclosed to the public, much of the essential details of the operation remain classified. Af-

ter disclosure of Monteilh's identity, Plaintiffs, three Muslim residents of Southern California, filed a putative class action against the FBI, the United States of America, and two FBI officers sued in their official capacities (together, the "Government") as well as five FBI agents sued in their individual capacities (collectively, "Defendants"). Plaintiffs allege that Defendants conducted an indiscriminate "dragnet" investigation and gathered personal information about them and other innocent Muslim Americans in Southern California based on their religion. In doing so, Plaintiffs allege that Defendants violated their constitutional and civil rights under the First Amendment Free Exercise Clause and Establishment Clause, the Religious Freedom Restoration Act ("RFRA"), the Fifth Amendment Equal Protection Clause, the Privacy Act, the Fourth Amendment, the Foreign Intelligence Surveillance Act ("FISA"), and the Federal Tort Claims Act ("FTCA"). Defendants currently move to dismiss Plaintiffs' claims and for summary judgment pursuant to Federal Rules of Civil Procedure 12 and 56 on various grounds, including the state secrets privilege. Defendants argue that all of Plaintiffs' claims, aside from their FISA and Fourth Amendment claims, must be dismissed because litigation of those claims would risk or require disclosure of certain evidence properly protected by the Attorney General's assertion of the state secrets privilege.

The Attorney General's privilege claim in this action requires the Court to wrestle with the difficult balance that the state secrets doctrine strikes between the fundamental principles of liberty, including judicial transparency, and national security. Although, as the Ninth Circuit aptly opined, "as judges we strive to honor *all* of these principles, there are times when exceptional cir-

cumstances create an irreconcilable conflict between them." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1073 (9th Cir. 2010), *cert. denied*, 131 S. Ct. 2442 (2011). "On those rare occasions, we are bound to follow the Supreme Court's admonition that 'even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake.'" *Id.* (quoting *United States v. Reynolds*, 345 U.S. 1, 11 (1953)). Such is the case here. After careful deliberation and skeptical scrutiny of the public and classified filings, the Court concludes that Plaintiffs' claims against Defendants, aside from their FISA claim, must be dismissed under the state secrets privilege.[1] Further litigation of those claims would require or unjustifiably risk disclosure of secret and classified information regarding the nature and scope of the FBI's counterterrorism investigations, the specific individuals under investigation and their associates, and the tactics and sources of information used in combating possible terrorist attacks on the United States and its allies. The state secrets privilege is specifically designed to protect against disclosure of such information that is so vital to our country's national security.

---

[1] Defendants' motions to dismiss Plaintiffs' FISA claim are discussed in the Court's separate, concurrently-issued Order. The Court finds that dismissal of Plaintiffs' FISA claim against the Government is warranted because sovereign immunity has not been waived. The Court, however, finds that Plaintiffs have alleged sufficient facts to state a FISA claim against the individual-capacity Agent Defendants, who are not entitled to qualified immunity at this stage of the proceeding based on the allegations pled in the First Amended Complaint.

II. BACKGROUND

The central subject matter of this case is a group of counterterrorism investigations by the FBI, known as "Operation Flex," which focused on fewer than 25 individuals and "was directed at detecting and preventing possible terrorist attacks." (Pub. Giuliano Decl. ¶ 11.) During the investigations, the FBI utilized Craig Monteilh as a confidential informant from 2006 to 2007. (*Id.* ¶¶ 6, 11.) "The goal of Operation Flex was to determine whether particular individuals were involved in the recruitment and training of individuals in the United States or overseas for possible terrorist activity." (*Id.* ¶ 11.) Plaintiffs allege that as part of Operation Flex, Defendants directed Monteilh to infiltrate mosques and indiscriminately collect information about Plaintiffs and other members of the Los Angeles and Orange County Muslim community because of their adherence to and practice of the religion of Islam from July 2006 to October 2007. (First Amended Complaint ("FAC") ¶¶ 1-3, 86, 167.)

The FBI has only acknowledged that Monteilh engaged in confidential source work and disclosed limited information concerning Monteilh's actions. (Pub. Giuliano Decl. ¶ 6.) For example, in an unrelated criminal proceeding in this district, *United States v. Niazi,* Case No. 8:09-cr-28-CJC(ANx), the FBI disclosed to the defendant Ahmadullah Niazi the content of the audio and video recordings containing conversations between him and Monteilh and others. (*Id.* ¶ 12.) The FBI also acknowledged in the *Niazi* case that Monteilh provided handwritten notes to the FBI and that it produced cer-

tain notes provided by Monteilh concerning Niazi. (*Id.*)[2] However, essential details regarding Operation Flex and Monteilh's activities have not been disclosed, and the Government asserts that this information "remains highly sensitive information concerning counterterrorism matters that if disclosed reasonably could be expected to cause significant harm to national security." (*Id.* ¶ 6.) The allegedly privileged information includes (i) the identities of the specific individuals who have or have not been the subject of counterterrorism investigations, (ii) the reasons why individuals were subject to investigation, including in Operation Flex, and their status and results, and (iii) the particular sources and methods used in obtaining information for counterterrorism investigations, including in Operation Flex. (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 6.) The Government provides a more fulsome discussion of the nondisclosed matters in its *ex parte, in camera* materials that include two classified declarations and a classified supplemental memorandum. (Dkt. Nos. 35, 36, 56.)

A. The Parties

Plaintiffs, Sheikh Yassir Fazaga, Ali Uddin Malik, and Yasser AbdelRahim (collectively, "Plaintiffs"), are resident members of the Muslim community in Southern California. (FAC ¶¶ 12-14.) Fazaga, a U.S. citizen born in Eritrea, has served as an "imam" or religious leader of the Orange County Islamic Foundation ("OCIF"), a

---

[2] With regard to these materials obtained by Monteilh, the FBI states that is it "presently assessing whether additional audio, video, or notes can be disclosed without risking disclosure of the privileged information . . . and [risking] significant harm to national security interests in protecting counterterrorism investigations." (Pub. Giuliano Decl. ¶ 12.)

mosque in Mission Viejo, California, and has lectured widely on topics of Islam and American Muslims. (*Id.* ¶¶ 12, 55-56.) Malik, a U.S. citizen born in Southern California, is a resident of Orange County and has regularly attended religious services at the Islamic Center of Irvine ("ICOI"), a mosque in Irvine, California. (*Id.* ¶¶ 13, 68-69.) AbdelRahim, a U.S. permanent resident from Egypt, has regularly attended religious services at the ICOI. (*Id.* ¶¶ 14, 80.)

The Government Defendants consist of the FBI and the United States of America as well as Robert Mueller, Director of the FBI, and Steven M. Martinez, Assistant Director in Charge of the FBI Los Angeles Field Office, sued in their official capacities. (*Id.* ¶¶ 15-17, 255.) Defendants also include five FBI agents, Kevin Armstrong, Paul Allen, J. Stephen Tidwell, Barbara Walls, and Pat Rose (collectively, "Agent Defendants"), who are sued in their individual capacities. (*Id.* ¶¶ 18-22.) Defendants Armstrong and Allen, who were both assigned to the Orange County area, were handlers for Monteilh and allegedly directed Monteilh to gather information on the Muslim community in Orange County and also supervised his purported surveillance activities. (*Id.* ¶¶ 18-19, 87.) Defendant Rose, who was assigned to the FBI's Santa Ana branch office, supervised the FBI's Orange County national security investigations and directly supervised Allen and Armstrong. (*Id.* ¶ 22.) Defendant Walls, the head of the FBI's Santa Ana branch office, directly supervised Allen, Armstrong, and Rose. (*Id.* ¶ 21.) Defendant Tidwell served as the Assistant Director in Charge of the FBI's Los Angeles Field Office from August 2005 to December 2007, and in that capacity, supervised operations in the Central District of California. (*Id.* ¶ 20.) Plaintiffs allege Tidwell

authorized the selection of Monteilh as an informant and directed the actions of Armstrong, Allen, Rose, Walls, and other agents in the handling of Monteilh. (*Id.*)

B. Operation Flex[3]

Plaintiffs allege many disturbing facts about Operation Flex and wrongdoing by Defendants. Sometime prior to July 2006, Plaintiffs allege that the FBI hired Monteilh to be a paid informant to covertly gather information about Muslims in the Irvine area. (FAC ¶ 48.) Monteilh became a Muslim convert, began to attend the ICOI and five of the other largest mosques in Orange County, and assumed the name Farouk al-Aziz. (*Id.* ¶¶ 49-50, 92.) Monteilh interacted with many members of the Muslim community in Southern California during the relevant time period, including Plaintiffs, as part of a "broader pattern of dragnet surveillance program that Monteilh engaged in at the behest of his FBI handlers," known as "Operation Flex," which referenced Monteilh's cover as a fitness instructor. (*Id.* ¶¶ 54-85, 86, 88.) Armstrong and Allen, who supervised all of Monteilh's work, informed Monteilh that Operation Flex was part of a broader surveillance program that went beyond his work. (*Id.* ¶ 88.) Defendants did not limit Monteilh to specific targets on which they wanted information, but "repeatedly made clear that they were interested simply in Muslims" and that he should gather "as much information on as many people in the Muslim community as possible," with heightened attention to

[3] The Court emphasizes that the facts regarding Operation Flex are only *allegations* from the FAC and do not constitute established facts or disclosures by Defendants. The FBI has neither confirmed nor denied that Monteilh collected information specifically in connection with any of the Plaintiffs or the putative class members.

particularly religious members and those who attracted Muslim youths. (*Id.* ¶¶ 89, 90, 98.) Plaintiffs allege that "[t]he central feature of the FBI agents' instructions to Monteilh was their directive that he gather information on Muslims, without any further specification," and indiscriminately gather information about them under the maximum that "everybody knows somebody" who may have some connection with the Taliban, Hezbollah, and Hamas. (*Id.* ¶¶ 89, 117.)

Over the course of Operation Flex, Plaintiffs allege that Armstrong and Allen sent Monteilh to conduct surveillance and audio recording in approximately ten mosques in Los Angeles and Orange County. (*Id.* ¶ 92.) Defendants provided Monteilh with surveillance tools, including sophisticated audio and video recording devices, such as key fobs with audio recording capability and a hidden camera outfitted to his shirt, to conduct an "indiscriminate surveillance" of Muslims, who were targeted "solely due to their religion." (*Id.* ¶¶ 86, 122, 124, 128.) Defendants gathered information about Plaintiffs and other members of the Muslim community through these devices and from extensive review of Monteilh's handwritten notes about all aspects of his daily interactions with Muslims. (*Id.* ¶ 122.) Plaintiffs allege that Armstrong and Allen were well aware that many of the surveillance tools they had given Monteilh were being used illegally without warrants. (*Id.* ¶ 136.)

Plaintiffs allege that the FBI Agents instructed Monteilh to utilize surveillance strategies aimed at gathering information on Muslims in an indiscriminate manner. (*Id.* ¶ 99.) The Agents' key directive was that Monteilh gather information from "anyone from any mosque

without any specific target, for the purpose of collecting as much information as possible about Muslims in the community." (*Id.* ¶ 114.) Armstrong and Allen instructed Monteilh to obtain information through various methods, including seizing every opportunity to meet people, obtain their contact information, and learn about their background and religious and political views. (*Id.* ¶ 101.) Monteilh did not limit surveillance to any particular group of people but instead socialized widely with different groups and individuals regardless of their ethnic origin or language. (*Id.* ¶¶ 102-103.) Armstrong and Allen further instructed Monteilh to gather information on Muslims' charitable givings, attend Muslim fundraising events, collect information on travel plans of Muslims in the community, attend lectures by Muslim scholars and other guest speakers, attend classes and dawn prayers at mosques, track followers of extremist jihadist websites, elicit people's views on extremist scholars and thinkers, work out with Muslims he met at a local gym, and gather any compromising information about Muslims that Defendants could use against them to persuade them to become informants. (*Id.* ¶¶ 105-16.) Plaintiffs allege that the consistent theme throughout these different surveillance gathering strategies was in Armstrong's and Allen's "expressed interest in gathering information only on Muslims," and their setting aside any non-Muslims who were identified through surveillance Monteilh performed. (*Id.* ¶ 120.)

Plaintiffs allege that through Monteilh, Defendants gathered information on Muslims and their associates consisting of hundreds of phone numbers and thousands of email addresses; background information on hundreds of individuals; hundreds of hours of video recordings that captured the interiors of mosques, homes, busi-

nesses, and the associations of Muslims; and thousands of hours of audio recordings of conversations as well as recordings of religious lectures, discussion groups, classes, and other Muslim religious and cultural events occurring in mosques. (*Id.* ¶¶ 2, 137.) Plaintiffs allege that the FBI's "dragnet investigation did not result in even a single conviction related to counterterrorism" because, unsurprisingly, "the FBI did not gather the information based on suspicion of criminal activity, but instead gathered the information simply because the targets were Muslim." (*Id.* ¶ 3.) Plaintiffs allege Monteilh discontinued working for Defendants as an informant around September 2007. (*Id.* ¶ 151.)

C. Disclosure of Monteilh's Identity

In February 2009, the FBI acknowledged that it had utilized Monteilh as a confidential informant during a criminal proceeding in the *Niazi* case. (Pub. Giuliano Decl. ¶ 11; FAC ¶¶ 155-59.)[4] Subsequent to this disclosure, Monteilh has provided numerous statements to the media discussing his purported activities on behalf of the FBI. (Pub. Giuliano Decl. ¶ 14; FAC ¶ 162.)[5] In January 2010, Monteilh also filed a civil lawsuit under 42 U.S.C. §§ 1983 and 1985 in this district against the FBI, its agents, and the City of Irvine in *Monteilh v. FBI*, Case No. 8:10-cv-102-JVS(RNBx). In that case, Monteilh made allegations related to his work as an FBI source in Operation Flex. (Pub. Giuliano Decl. ¶ 14; FAC ¶ 164.) The FBI has neither confirmed nor denied

---

[4] This Court dismissed the *Niazi* indictment without prejudice on September 30, 2010. (Case No. 8:09-cr-28-CJC (ANx), Ct. Order, Dkt. No. 40, Sept. 30, 2010.)

[5] *See, e.g.*, Jerry Markon, *Tension Grows between Calif. Muslims, FBI after Informant Infiltrates Mosque*, WASH. POST (Dec. 5, 2010).

any of Monteilh's public allegations concerning his work for the agency, and the FBI maintains that Monteilh's allegations do not constitute a disclosure or confirmation by the FBI of any information concerning his activities as an informant. (Pub. Giuliano Decl. ¶ 14; FAC ¶ 164.) In this case, Monteilh has submitted a declaration, dated April 23, 2010, in support of Plaintiffs' opposition to Defendants' motions to dismiss in which he makes allegations regarding his work for the FBI in Operation Flex similar to those asserted in the FAC. (Dkt. No. 66; FAC ¶ 167.)

D. The Lawsuit

On February 22, 2011, Plaintiffs filed the instant suit against the FBI and its officers and agents. (Dkt. No. 1.) On August 1, 2011, the FBI, Mueller, and Martinez moved to dismiss the Complaint and for summary judgment on the grounds, *inter alia,* that certain evidence needed to litigate Plaintiffs' claims is properly protected by the Attorney General's assertion of the state secrets privilege. (Dkt. No. 32.) In support of their privilege claim, they submitted for *ex parte, in camera* review by the Court (i) a classified declaration of Mark F. Giuliano, FBI Assistant Director, Counterterrorism Division and (ii) a classified supplemental memorandum. (Dkt. Nos. 35, 36.) The Agent Defendants also separately moved to dismiss the Complaint. (Dkt. Nos. 41-42.) Shortly thereafter, Plaintiffs moved *ex parte* to stay the Court's review of the classified filings until after its consideration of whether the state secrets argument would apply in this case as a matter of law. (Dkt. No. 39.) Plaintiffs argued that such a ruling would prevent the Court from unnecessarily reviewing information that could be highly prejudicial to Plaintiffs and not properly subject

to consideration by the Court. (Pls. Ex Parte App., at 8.) The Court denied Plaintiffs' *ex parte* application because the Court determined that there was no legal bar to its review of the classified submissions and because it was confident that its independent evaluation would not be compromised by the contents of those submissions. (Ct. Order, Dkt. No. 46, Aug. 11, 2011.)

On September 13, 2011, Plaintiffs filed the operative FAC, adding a claim under the FTCA against the United States. (Dkt. No. 49.) Plaintiffs assert a total of eleven causes of action against Defendants: (1) violation of the First Amendment Establishment Clause under *Bivens* and 28 U.S.C. § 1331 (against all Defendants except the FBI and United States); (2) violation of the First Amendment Establishment Clause under 42 U.S.C. § 1985(3) and 28 U.S.C. § 1343 (against Agent Defendants); (3) violation of the First Amendment Free Exercise Clause under *Bivens* and 28 U.S.C. § 1331 (against all Defendants except the FBI and United States); (4) violation of the First Amendment Free Exercise Clause under 42 U.S.C. § 1985(3) and 28 U.S.C. § 1343 (against Agent Defendants); (5) violation of RFRA, 42 U.S.C. § 2000bb-1 (against all Defendants); (6) violation of the Fifth Amendment Equal Protection Clause under *Bivens* and 28 U.S.C. § 1331 (against all Defendants except the FBI and United States); (7) violation of the Equal Protection Clause under 42 U.S.C. § 1985(3) and 28 U.S.C. § 1343 (against Agent Defendants); (8) violation of the Privacy Act, 5 U.S.C. § 552a(a)-(*l*) (against the FBI); (9) violation of the Fourth Amendment under *Bivens* and 28 U.S.C. § 1331 (against the FBI and United States); (10) violation of FISA, 50 U.S.C. § 1810 (against all Defendants); and (11) invasion of privacy, violation of Cal. Civ. Code § 52.1, and intentional infliction

of emotion distress under the FTCA, 28 U.S.C. §§ 1346(b), 2671, *et seq.* (against the United States).[6] Plaintiffs request damages as well as injunctive relief in the form of the destruction or return of any information gathered through Operation Flex. Plaintiffs further seek certification of "[a]ll individuals targeted by Defendants for surveillance or information-gathering through Monteilh and Operation Flex, on account of their religion, and about whom the FBI thereby gathered personally identifiable information." (FAC ¶ 219.)

On November 4, 2011, the Government moved to dismiss the FAC and for summary judgment pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(6), and 56. (Dkt. No. 55.) The Government moves to dismiss all of Plaintiffs' claims, aside from the FISA and Fourth Amendment claims, on the grounds that, *inter alia,* litigation of these claims would risk or require the disclosure of certain evidence properly protected by the Attorney General's assertion of the state secrets privilege. In support of their privilege claim, the Government relies on its previously-filed public declaration from the Attorney General, Eric H. Holder, dated July 29, 2011, (Dkt. No. 32-3), and a public declaration from Mark Giuliano, dated July 25, 2011, (Dkt. No. 33). The Government also relies on its previously-lodged, August 1, 2011 *in camera* filings, the classified declaration of Giuliano and the classified supplemental memorandum, (Dkt. Nos. 35, 36). In addition, the Government lodged a classified supplemental declaration of Giuliano on November

---

[6] For claims 1, 3, 6, and 9, Plaintiffs assert claims for damages under *Bivens* against individual-capacity Agent Defendants and assert claims for injunctive relief under Section 1331 against the official-capacity Defendants. (*See* FAC ¶ 226 n.37.)

4, 2011, which provided a status update on certain investigations discussed in the classified Giuliano Declaration. (Dkt. No. 56.)

Defendants Tidwell and Walls separately moved to dismiss claims against them under Federal Rule of Civil Procedure 12(b)(6). (Dkt. No. 58.) Tidwell and Walls argue, in part, that the Government's assertion of the state secrets privilege mandates dismissal of Counts 1 through 7. (Tidwell/Walls Br., at 9-12.) Defendants Rose, Armstrong, and Allen also moved to dismiss the FAC under Rule 12(b)(6) and joined in the motions to dismiss filed by the Government and Defendants Tidwell and Walls. (Dkt. No. 57.) On December 23, 2011, Plaintiffs opposed the Government's motion and filed a combined opposition to the Agent Defendants' motions to dismiss. (Dkt. Nos. 63, 64.) Defendants filed replies in support of their respective motions to dismiss on January 20, 2012. (Dkt. Nos. 69-71.) After granting the parties' requests for continuances of the hearing on Defendants' motions to dismiss, the Court heard extended oral arguments on the motions from the parties' counsel on August 14, 2012.

III. LEGAL STANDARD

A. The State Secrets Doctrine

"The Supreme Court has long recognized that in exceptional circumstances courts must act in the interest of the country's national security to prevent disclosure of state secrets, even to the point of dismissing a case entirely." *Jeppesen Dataplan,* 614 F.3d at 1077 (citing *Totten v. United States,* 92 U.S. 105, 107 (1875)). Created by federal common law, the state secrets doctrine bars litigation of an action entirely or excludes certain evidence because the case or evidence risks disclosure

of "state secrets"—that is, "matters which, in the interest of national security, should not be divulged." *Reynolds,* 345 U.S. at 10, 73 S. Ct. 528. Although developed at common law, the state secrets doctrine also "performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities." *El-Masri v. United States,* 479 F.3d 296, 303 (4th Cir. 2007). At the same time, the state secrets doctrine does not represent an abdication of judicial control over access to the courts, as the judiciary is ultimately tasked with deciding whether the doctrine properly applies to a particular case. *Id.* at 312. The state secrets doctrine thus attempts to strike a difficult balance between the Executive's duty to protect national security information and the judiciary's obligation to preserve judicial transparency in its search for the truth. *Id.* at 303-305.

There are two modern applications of the state secrets doctrine: (1) a justiciability bar that forecloses litigation altogether because the very subject matter of the case is a state secret (the "*Totten* bar") and (2) an evidentiary privilege that excludes certain evidence because it implicates secret information and may result in dismissal of claims (the "*Reynolds* privilege"). *Jeppesen Dataplan,* 614 F.3d at 1077-80. While distinct, the *Totten* bar and the *Reynolds* privilege converge in situations where the government invokes the privilege—as it may properly do—before waiting for an evidentiary dispute to arise during discovery or trial. *Id.* at 1080 ("The privilege may be asserted at any time, even at the pleading stage."). The privilege indisputably may be raised with respect to discovery requests seeking allegedly privileged information or to prevent disclosure of such

information in a responsive pleading. *Id.* at 1081. Alternatively, "the government may assert a *Reynolds* privilege claim prospectively, even at the pleading stage, rather than waiting for an evidentiary dispute to arise during discovery or trial." *Id.* In such circumstances, the *Totten* bar necessarily informs the *Reynolds* privilege in a "continuum of analysis." *Al-Haramain Islamic Found., Inc. v. Bush,* 507 F.3d 1190, 1201 (9th Cir. 2007).

1. The Totten Bar

The Supreme Court in *Totten v. United States* articulated the general principle that "public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential." 92 U.S. at 107. The *Totten* bar is a categorical bar "where the very subject matter of the action . . . [is] a matter of state secret," such that the action is "dismissed on the pleadings without ever reaching the question of evidence since it [is] so obvious that the action should never prevail over the privilege." *Reynolds,* 345 U.S. at 11 n.26, 73 S. Ct. 528; *accord Jeppesen Dataplan,* 614 F.3d at 1077-78; *see also Al-Haramain,* 507 F.3d at 1197 ("[W]here the very subject matter of a lawsuit is a matter of state secret, the action must be dismissed without reaching the question of evidence."). The purpose of the *Totten* bar is not merely to defeat the asserted claims, but to foreclose judicial inquiry altogether. *Tenet v. Doe,* 544 U.S. 1, 6 n.4 (2005); *Jeppesen Dataplan,* 614 F.3d at 1078.

The Supreme Court has very sparingly applied this bar to preclude judicial review of an action entirely. *See Totten,* 92 U.S. at 106-107 (barring suit by Civil War spy against the United States for alleged failure to pay for

espionage services because the case was predicated on the existence of an undisclosed contract for secret services with the government); *Weinberger v. Catholic Action of Hawaii/Peace Educ. Project,* 454 U.S. 139, 146-47 (1981) (holding action against the United States Navy exceeded judicial scrutiny based on state secrets because it implicated information regarding nuclear weapons storage that the Navy could not admit or deny); *Tenet,* 544 U.S. at 8-10, 125 S. Ct. 1230 (precluding judicial review of action by former Cold War spies against the Central Intelligence Agency for allegedly reneging on promise to pay for espionage services because plaintiffs' relationship with the government was state secrets). Beyond these three cases, the Supreme Court has not provided further guidance on what subject matters would constitute state secrets. The Ninth Circuit in *Jeppesen,* however, declined to interpret the *Totten* bar as only applying to certain types of cases, such as those involving covert espionage agreements, but emphasized that "the *Totten* bar rests on a general principle that extends beyond that specific context" and applies "'where the very subject matter of the action' is 'a matter of state secret.'" 614 F.3d at 1078-79 (quoting *Reynolds,* 345 U.S. at 11 n.26, 73 S. Ct. 528). The *El-Masri* court further clarified that "[t]he controlling inquiry is not whether the general subject matter of an action can be described without resort to state secrets"; rather, it must be ascertained "whether an action can be *litigated* without threatening the disclosure of such state secrets." *El-Masri,* 479 F.3d at 308. "Thus, for purposes of the state secrets analysis, the 'central facts' and 'very subject matter' of an action are those facts that are essential to prosecuting the action or defending against it." *Id.*

2. The Reynolds Privilege

The second application of the state secrets doctrine is an evidentiary privilege against revealing state secrets. *Jeppesen Dataplan,* 614 F.3d at 1079. Derived from *United States v. Reynolds,* this privilege applies when the court is satisfied "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Reynolds,* 345 U.S. at 10, 73 S. Ct. 528; *see also id.* at 10-11, 73 S. Ct. 528 (finding that the government made a sufficient showing of privilege, "under circumstances indicating a reasonable possibility that military secrets were involved," to cut off demand for an accident investigation report of an aircraft testing secret electronic equipment). A successful assertion of the *Reynolds* privilege will remove the privileged evidence from the case. *Jeppesen Dataplan,* 614 F.3d at 1079. In some instances, however, "the assertion of the privilege will require dismissal because it will become apparent during the *Reynolds* analysis that the case cannot proceed without privileged evidence, or that litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Id.* The Ninth Circuit in *Jeppesen Dataplan* applied the *Reynolds* privilege to dismiss an action brought by foreign nationals who were allegedly transported in secret to other countries where they were detained and interrogated under the Central Intelligence Agency's ("CIA") extraordinary rendition program. 614 F.3d at 1085-90. The Ninth Circuit held that dismissal under the state secrets privilege was required under *Reynolds* because there was no feasible way to litigate the defendant's liability without creating "an unjustifiable risk of divulging

state secrets" related to the CIA's secret intelligence activities. *Id.* at 1087. When such dismissal is required, the *Reynolds* privilege converges with the *Totten* bar. *Id.* at 1083.

An analysis of claims under the *Reynolds* privilege involves three steps. First, the court must ascertain whether the procedural requirements for invoking the privilege, consisting of a formal claim by the government, have been satisfied. *Id.* at 1080. Second, the court must independently determine whether the information is privileged. *Id.* Third, the court must determine how the case should proceed in light of the successful privilege claim. *Id.* Once the privilege is properly invoked, and the court is satisfied as to the danger of disclosing state secrets, the privilege is absolute. *Kasza v. Browner,* 133 F.3d 1159, 1166 (9th Cir. 1998); *see also Reynolds,* 345 U.S. at 11, 73 S. Ct. 528 ("[E]ven the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake."); *In re United States,* 872 F.2d 472, 476 (D.C. Cir. 1989) ("No competing public or private interest can be advanced to compel disclosure [of privileged information]." (citation and quotes omitted)). This is because, in determining whether the privilege applies to a particular case, "the balance has already been struck in favor of protecting secrets of state over the interest of a particular litigant." *In re United States,* 872 F.2d at 476 (citation and quotes omitted). The Supreme Court has therefore cautioned that the privilege "is not to be lightly invoked," and must be applied no more often or extensively than necessary. *Reynolds,* 345 U.S. at 7-8, 73 S. Ct. 528; *see also Jeppesen Dataplan,* 614 F.3d at 1080.

B. Threshold Considerations

Plaintiffs raise two threshold issues with regard to whether the state secrets doctrine may apply in this case, neither of which are persuasive. First, Plaintiffs argue that FISA preempts the state secrets privilege. Plaintiffs insist that because most, if not all, of the conduct at issue in this case involves electronic surveillance in the name of foreign intelligence gathering in the domestic context, the Court should adhere to the procedures that Congress has set for the treatment of secret evidence in FISA.[7] (Pls. Opp'n to Gov't, at 20-21, 26-31.) The Court disagrees. As a preliminary matter, the question of whether FISA preempts the state secrets privilege is not at issue because Defendants have not moved to dismiss the FISA claim on privilege grounds. Moreover, even if FISA preempts the state secrets privilege with respect to a FISA claim, as ruled by the Northern District of California in *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109, 1120 (N.D. Cal. 2008),[8] Plaintiffs cite no authority for the proposition that FISA also preempts non-FISA claims. Nor has the Court found any statute, including the language of FISA, or case law supporting an expansive application of FISA to Plaintiffs' non-FISA claims in this case. Plaintiffs rely on *In re National Security Agency,* 564

---

[7] *See* the Court's concurrently-filed Order, which discusses the FISA claim in detail.

[8] The Court in *In re National Security* determined that "FISA should displace federal common law rules such as the state secrets privilege with regard to matters within FISA's purview." 564 F. Supp. 2d at 1120. As the Government does not move to dismiss the FISA claim on the basis of state secrets, the Court need not and does not decide at this time whether FISA preempts the state secrets privilege with respect to a FISA claim.

F. Supp. 2d at 1118, for the proposition that FISA preempts the state secrets privilege in cases, as here, which involve electronic surveillance undertaken in the name of national security. (Pls. Opp'n to Gov't, at 26, 29). However, the court in that case clarified that "FISA does not preempt the state secrets privilege as to matters that are not within FISA's purview,"—that is, "activities [that] include foreign intelligence surveillance." *In re National Security Agency,* 564 F. Supp. 2d at 1118. In the present action, however, the central subject matter is Operation Flex, a group of counterterrorism investigations that extend well beyond the purview of electronic surveillance as discussed in the Government's public and classified filings. Plaintiffs' non-FISA claims also rely upon allegations far broader in scope than allegations upon which the FISA claim is predicated, and litigating those non-FISA claims will require information, including privileged evidence, beyond that contemplated by FISA. (*See infra* Part IV.C.)

Second, Plaintiffs argue that the Constitution prohibits dismissal of this case on state secret grounds because they seek injunctive relief from on-going constitutional violations. (Pls. Opp'n to Gov't, at 20, 40-51.) This argument, likewise, is unsupported by any authority, let alone Ninth Circuit or Supreme Court precedent. The principles of the state secrets doctrine make clear that it is analyzed and applied to cases irrespective of the types of claims or relief sought. *See Tenet,* 544 U.S. at 8, 125 S. Ct. 1230 ("[P]ublic policy forbids the maintenance of *any suit* in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential." (quoting *Totten,* 92 U.S. at 107)); *Kasza,* 133 F.3d at 1166 ("Once the privilege is properly invoked and the court is satisfied as to the dan-

ger of divulging state secrets, the privilege is absolute . . . "); *Jeppesen Dataplan*, 614 F.3d at 1081 ("If this standard [for privilege] is met, the evidence is absolutely privileged, irrespective of the plaintiffs' countervailing need for it."). In fact, in *Al-Haramain*, the Ninth Circuit found that the state secrets privilege applied to and warranted dismissal of constitutional claims involving requests for injunctive relief. 507 F.3d at 1205. In that case, Al-Haramain Islamic Foundation, a designated terrorist organization, and two of its attorneys brought suit against the government in connection with the government's Terrorist Surveillance Program. 507 F.3d at 1193. The plaintiffs in that case alleged that they were subject to warrantless electronic surveillance in violation of FISA and various provisions of the Constitution. *Id.* In addition to a request to enjoin further warrantless surveillance, the plaintiffs sought the same injunctive relief as Plaintiffs here do—disclosure and/or destruction of information and records acquired from allegedly unlawful surveillance—and also similarly alleged violations under the First and Fourth Amendments. *Al-Haramain Islamic Found., Inc. v. Bush*, 451 F. Supp. 2d 1215, 1218 (D. Or. 2006), *rev'd and remanded by Al-Haramain*, 507 F.3d 1190. The Ninth Circuit in *Al-Haramain* found dismissal of the action appropriate under the *Reynolds* privilege because the defendant could not establish standing without the privileged information. 507 F.3d at 1205.[9] Accordingly, the Court finds that the state secrets doctrine may properly be considered in this case.

---

[9] Plaintiffs' argument is additionally misplaced because, even assuming that their argument regarding constitutional claims for injunctive relief had merit, it would be inapplicable as to their claims for damages against Defendants.

IV. APPLICATION OF THE STATE SECRETS DOCTRINE

The Government requests dismissal of all of Plaintiffs' claims against Defendants, aside from the FISA and Fourth Amendment claims, under the *Reynolds* privilege. The Government argues that dismissal of these claims under the state secrets privilege is appropriate because it has satisfied the procedural requirements for invoking the privilege and further litigation of the action would risk or require the disclosure of state secrets related to Operation Flex. More specifically, the Government contends that because Plaintiffs' claims are premised on their core allegation that Defendants conducted an indiscriminate religion-based investigation, any rebuttal against this allegation would risk or require disclosure of privileged information—whom and what the FBI was investigating under Operation Flex and why—in order to establish that the investigation was properly predicated and focused. (Gov't Br., at 5-6, 45-53.) The Court agrees. As discussed more fully below, because further litigation of this action would require or, at the very least, create an unjustifiable risk of disclosure of state secrets, the Court finds that dismissal of Plaintiffs' claims, aside from their FISA claim, is required under the *Reynolds* privilege.

A. Procedural Requirements

The *Reynolds* privilege may only be asserted by the government, and a private party can neither claim nor waive the privilege. *Jeppesen Dataplan,* 614 F.3d at 1080; *Reynolds,* 345 U.S. at 7, 73 S. Ct. 528. The government cannot invoke the privilege lightly, especially where it seeks not merely to preclude the production of certain evidence, but to obtain dismissal of the action en-

tirely. *Jeppesen Dataplan,* 614 F.3d at 1080. There are several mechanisms to ensure that the *Reynolds* privilege is invoked no more than is necessary. *Id.* First, "[t]here must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Reynolds,* 345 U.S. at 7-8, 73 S. Ct. 528. "This certification is fundamental to the government's claim of privilege," as the decision to invoke the privilege must "'be a serious, considered judgment, not simply an administrative formality.'" *Jeppesen Dataplan,* 614 F.3d at 1080 (quoting *United States v. W.R. Grace,* 526 F.3d 499, 507-508 (9th Cir. 2008) (en banc)). The formal claim must "reflect the certifying official's *personal* judgment," and be presented in "sufficient detail" to permit the court "to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Id.* at 1080.

Second, even before invoking the privilege in court, the government must adhere to its own State Secrets Policy, promulgated by the Obama administration in a memorandum by the Attorney General in September 2009, effective October 1, 2009. (Holder Decl. ¶ 12 & Exh. 1 [State Secrets Policy]); *see also Jeppesen Dataplan,* 614 F.3d at 1077. The Policy outlines the legal standard for invoking the privilege: the government will assert and defend an assertion of the state secrets privilege in litigation "when a government department or agency seeking to assert the privilege makes a sufficient showing that assertion of the privilege is necessary to protect information the unauthorized disclosure of which reasonably could be expected to cause significant harm to the national defense or foreign relations ("national security") of the United States." (Holder Decl.,

Exh. 1 ¶ 1(A).) The privilege must also be "narrowly tailored," such that the "privilege should be invoked only to the extent necessary to protect against the risk of significant harm to national security." (*Id.* ¶ 1(B).) The Policy further sets limitations for invoking the privilege, including not defending an invocation of the privilege to "conceal violations of the law, inefficiency, or administrative error"; to "prevent embarrassment to a person, organization, or agency of the United States government"; or to "prevent or delay the release of information the release of which would not reasonably be expected to cause significant harm to national security." (*Id.* ¶ 1(C).) The Policy further outlines the initial procedure for invoking the privilege, which includes sufficient evidentiary support and recommendation from the Assistant Attorney General; evaluation, consultation, and recommendation by a state secrets review committee; and approval by the Attorney General. (*Id.* ¶¶ 2-4.)

The Government has properly invoked the state secrets privilege. The Government has submitted a public declaration from Eric Holder in his capacity as the Attorney General and head of the Department of Justice. The Attorney General has made a formal assertion of the state secrets privilege after personal consideration of the public and classified materials at the request of the director of the FBI: "After careful and actual personal consideration of the matter, I have concluded that disclosure of the three categories of information described below and in more detail in the classified Giuliano Declaration could reasonably be expected to cause significant harm to the national security, and I therefore formally assert the state secrets privilege over this information." (Holder Decl. ¶ 3.) The Attorney General also avers that the requirements for an assertion and

defense of the state secrets privilege have been satisfied in accordance with the State Secrets Policy. (*Id.* ¶ 12.)[10]

B. Independent Evaluation of the Privilege Claim

After a court determines that the privilege has been properly invoked, it then "'must make an independent determination whether the information is privileged.'" *Jeppesen Dataplan,* 614 F.3d at 1080, 1081 (quoting *Al-Haramain,* 507 F.3d at 1202). "The court must sustain a claim of privilege when it is satisfied, 'from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged.'" *Id.* at 1081 (quoting *Reynolds,* 345 U.S. at 10, 73 S. Ct. 528). "The Executive bears the burden of satisfying a reviewing court that the *Reynolds* reasonable-danger standard is met." *El-Masri,* 479 F.3d at 305. The government cannot satisfy this burden by the mere conclusory assertion that the standard has been met. *El-Masri,* 479 F.3d at 312. "Simply saying 'mili-

[10] The Court cannot and does not comment on whether the Government has properly adhered to its State Secrets Policy, as this is internal to the Executive branch, and the Policy does not create a substantive or procedural right enforceable at law or in equity against the Government. (*See* Holder Decl., Exh. 1 ¶ 7.) However, the Court does observe that the Government has narrowly tailored its assertion of the privilege by moving on other grounds before invoking the privilege and has done so with restraint. (See Gov't Br., at 3-7.) While the Court has considered Defendants' initial grounds for dismissal before analyzing the state secrets privilege, the Court believes they are limited and do not entirely warrant dismissal of Plaintiffs' claims. In contrast, the Court finds that all of Plaintiffs' claims, aside from their FISA claim, should be dismissed under the *Reynolds* privilege. For this reason and for the sake of judicial economy, the Court limits its discussion to the state secrets doctrine in this Order and the FISA claim in the Court's concurrently-issued Order.

tary secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege." *Al-Haramain,* 507 F.3d at 1203. Rather, the government must provide "[s]ufficient detail" to enable the court to conduct a meaningful examination. *Id.* In some instances, a formal privilege claim asserted in a declaration may suffice, while in others, the court may conduct an *in camera* examination of the allegedly privileged information. *El-Masri,* 479 F.3d at 305. "The degree to which such a reviewing court should probe depends in part on the importance of the assertedly privileged information to the position of the party seeking it." *Id.*; *see also Reynolds,* 345 U.S. at 11, 73 S. Ct. 528 ("In each case, the showing of necessity which is made will determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate.") At the same time, the Court must make this determination "without forcing a disclosure of the very thing the privilege is designed to protect." *Reynolds,* 345 U.S. at 8, 73 S. Ct. 528. "If this standard is met, the evidence is absolutely privileged, irrespective of the plaintiffs' countervailing need for it." *Jeppesen Dataplan,* 614 F.3d at 1081.

Here, the Government asserts the privilege over three categories of information related to Operation Flex as described in their public and classified filings: (i) subject identification, (ii) reasons for counterterrorism, and (iii) sources and methods. First, the FBI seeks to protect "[i]nformation that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation, including in Operation Flex." (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 15.) Second, the FBI seeks to protect

"[i]nformation that could tend to reveal the initial reasons (*i.e.,* predicate) for an FBI counterterrorism investigation of a particular person (including in Operation Flex), any information obtained during the course of such an investigation, and the status and results of the investigation. This category includes any information obtained from the U.S. Intelligence Community related to the reasons for an investigation." (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 15.) Third, the FBI seeks to protect "[i]nformation that could tend to reveal whether particular sources and methods were used in a counterterrorism investigation of a particular subject, including in Operation Flex," and "previously undisclosed information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative sources and methods were used in a counterterrorism investigation of a particular person, the reasons such methods were used, the status of the use of such sources and methods, and any results derived from such methods." (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 15.)

Beyond the Government's descriptions of these categories of information in its public declarations, the Court heavily relies upon the classified declarations and supplemental memorandum to determine whether disclosure of the information described above could reasonably be expected to cause significant harm to national security. In making this determination, the Court assumes the "'special burden to assure itself that an appropriate balance is struck between protecting national security matters and preserving an open court system.'" *Jeppesen Dataplan,* 614 F.3d at 1081 (quoting *Al-Haramain,* 507 F.3d at 1203); *see also El-Masri,* 479 F.3d at 304 ("This inquiry is a difficult one, for it pits the

judiciary's search for truth against the Executive's duty to maintain the nation's security."). On the one hand, the Court "acknowledge[s] the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find [itself] second guessing the Executive in this arena." *Jeppesen Dataplan,* 614 F.3d at 1081-82; *see also El-Masri,* 479 F.3d at 305 ("In assessing the risk that such a disclosure [of state secrets] might pose to national security, a court is obliged to accord the 'utmost deference' to the responsibilities of the executive branch.") (quoting *United States v. Nixon,* 418 U.S. 683, 710 (1974)). On the other hand, "'the state secrets doctrine does not represent a surrender of judicial control over access to the courts.'" *Jeppesen Dataplan,* 614 F.3d at 1082 (quoting *El-Masri,* 479 F.3d at 312); *see also Reynolds,* 345 U.S. at 9-10, 73 S. Ct. 528 ("Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers.") Rather, the Court has the obligation "to ensure that the state secrets privilege is asserted no more frequently and sweepingly than necessary," by critically examining the instances of its invocation, *Ellsberg v. Mitchell,* 709 F.2d 51, 58 (D.C. Cir. 1983), with "a very careful, indeed a skeptical, eye, and not to accept at face value the government's claim or justification of privilege," *Al-Haramain,* 507 F.3d at 1203. *See also Jeppesen Dataplan,* 614 F.3d at 1082. But the Court cannot delve so deeply that it discloses the very information the privilege is meant to protect. *Reynolds,* 345 U.S. at 8, 73 S. Ct. 528 ("Too much judicial inquiry into the claim of privilege would force disclosure of the thing the privilege is meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses.")

The Court has thoroughly and skeptically examined the Government's public and classified submissions. In particular, the Court has critically scrutinized the Attorney General's classified declarations and the classified memorandum—which are comprehensive and detailed—since they were submitted for the Court's *ex parte, in camera* review in August and November 2011. The Court is convinced that the subject matter of this action, Operation Flex, involves intelligence that, if disclosed, would significantly compromise national security. The Court is further convinced that litigation of this action would certainly require or, at the very least, greatly risk disclosure of secret information, such that dismissal at this stage of the proceeding is required. This is because, as described more fully below, the Government will inevitably need the privileged information to defend against Plaintiffs' core allegation that Defendants conducted an indiscriminate "dragnet" investigation and gathered information on Plaintiffs and Muslims in Southern California based on their religion. (*See infra* Part IV.C.)

In their Opposition, Plaintiffs argue that the Government's first category of information is not privileged because everyone who had contact with Monteilh already knows that they were targeted for investigation. (Pls. Opp'n to Gov't, at 31-32.) However, aside from the general information about Operation Flex and the identity of Monteilh as an informant, the Government has not confirmed or denied the identities of the fewer than 25 individuals who were under investigation. Plaintiffs further argue that because the Government has not explicitly invoked the *Totten* bar, it has effectively conceded that the very subject matter of this action is *not* a state secret. (*Id.* at 23.) But while some of the general facts

of Operation Flex are public knowledge, the facts required to *litigate* the action—*e.g.,* to defend against Plaintiffs' claims of indiscriminate targeting of Muslims—requires disclosure of information that is classified and privileged. *El Masri,* 479 F.3d at 308 ("[F]or purposes of the state secrets analysis, the 'central facts' and 'very subject matter' of an action are those facts that are essential to prosecuting the action or defending against it.") Plaintiffs' position to the contrary implies an overly rigid understanding of the difference between the *Totten* bar and *Reynolds* privilege that is inconsistent with the Ninth Circuit's application of the state secrets doctrine. As the *Jeppesen* court indicated, the state secrets analysis under the *Totten* bar converges with its progeny when, as here, the Government requests dismissal at the pleading stage because defense against plaintiff's claims requires privileged evidence or further litigation of the case would present an unacceptable risk of disclosing state secrets. *Jeppesen Dataplan,* 614 F.3d at 1083. (*See infra* Part IV.C.)

While the Court cannot describe the specific contents of the classified materials—as this would thwart the very purpose of the privilege claim—the Court can make the following observations. In the context of a counterterrorism investigation, subject identification may include information about persons residing in the United States or abroad, such as Afghanistan, Lebanon, the Palestinian Territories, Yemen, and other regions in the Middle East, whom law enforcement has and has not decided to investigate depending on their nexus to terrorist organizations, such as al Qaeda, the Taliban, Hezbollah, and Hamas. Subjects and their associates may also be investigated because they are suspected of or involved in the recruitment, training, indoctrination, or

radicalization of individuals for terrorist activities or fundraising for terrorist organizations. More directly, individuals subjected to counterterrorism investigations may be involved in plotting terrorist attacks. In the nearly eleven years that have passed since September 11, 2001, Islamic extremists have continued to plot and attempt to carry out numerous terrorist attacks both on U.S. soil and abroad against U.S. targets and allies. Such attacks are not abstract events born out of fear, but are real and insidious. The Daily Beast reported that as of September 8, 2011, "there have been at least 45 jihadist terrorist-attack plots against Americans since 9/11—each of them thwarted by a combination of intelligence work, policing and citizen participation." John Avlon, *Forty-Five Foiled Terror Plots Since 9/11,* Daily Beast (Sept. 8, 2011), http://www.thedailybeast.com/articles/2011/09/08/9-11-anniversary-45-terror-plots-foiled-in-last-10-years.html. The article notes that "these are just the plotted attacks that we know about through public documentation" and that "the real number of credible plots is no doubt much higher." *Id.* Examples of recent, known terrorist attempts include the September 2009 scheme by Najibullah Zazi, who was arrested for plotting to attack the New York City subway system, as well as the December 2009 failed attempt by Umar Farouk Abdulmutallab to bomb Northwest Flight 253 to Chicago and the May 2010 failed attempt of Faisal Shazad to detonate a car bomb in Times Square. (*See* Pub. Giuliano Decl. ¶¶ 8-9.) Subjects and their associates may be further investigated because they have ties to homegrown violent extremists who do not necessarily receive guidance from terrorist groups overseas but may be inspired by the global jihadist movement to commit violent acts inside the United States. Such was the

case for a group of armed men who were arrested before they could execute their plot to kill people inside a military recruiting center in Santa Monica, California, on September 11, 2005, and then later open fire on families outside of temple during Yom Kippur in West Los Angeles. (*See id.* ¶ 10.)

Disclosure of subjects under investigation would undoubtedly jeopardize national security. This is because persons under investigation would be alerted to the FBI's interest in them and cause them to flee, destroy evidence, or alter their conduct so as to avoid detection, which would seriously impede law enforcement's and intelligence officers' ability to determine their location or gain further intelligence on their activities. (Holder Decl. ¶ 6; Pub. Giuliano Decl. ¶ 23.) Disclosure of those *not* under investigation by the FBI is, likewise, dangerous because individuals who desire to commit terrorist acts may then be motivated to do so upon discovering that they are not being monitored. Information about who is being investigated while the status of others are unconfirmed may be manipulated by individuals and terrorist groups to discover whether they or any of their members are being investigated. (Holder Decl. ¶ 7; Pub. Giuliano Decl. ¶ 24.)

The second and third categories of information necessarily overlap with the first. The reasons and results of counterterrorism investigations may include the identities of human sources, such as confidential informants or undercover agents and officers (other than Monteilh); existent or suspected links between individuals and terrorist organizations; the results of surveillance efforts; and information shared among law enforcement and other government agencies. This category of evidence

will also likely involve information about the status of the investigation—whether a particular investigation is open or closed—or the substantive details of the investigations themselves. With regard to the third category, this is likely to include information similar to the first and second categories, such as what, if any, confidential human sources besides Monteilh were used; whether court-authorized searches or surveillance occurred, such as wire taps and monitoring of electronic communication; whether the investigations involved undercover activity or physical surveillance; and whether interviews with suspects and their associates were conducted. The disclosure of the reasons and results of counterterrorism investigations would unquestionably compromise national security because it would reveal to those involved in plotting terrorist activities what the FBI knows and does not know about their plans and thereby enable them to evade detection. (Holder Decl. ¶ 9; Pub. Giuliano Decl. ¶ 29.) The disclosure of the methods and sources would endanger national security because it could reveal the identities of particular subjects and the steps taken by the FBI in counterterrorism matters, thereby effectively disclosing a road map to adversaries on how the FBI detects and prevents terrorist activities. (Holder Decl. ¶ 10; Pub. Giuliano Decl. ¶ 31.)

Aside from these explanations, the Court cannot and need not give any further details with regard to the contents of the classified materials. *See Kasza*, 133 F.3d at 1169 (concluding that *in camera* review of classified declarations "was an appropriate means to resolve the applicability and scope of the state secrets privilege," and "[n]o further disclosure or explanation is required"). The Court, however, is thoroughly convinced that the

Government has described, in sufficient detail, the nature of the privileged information and reasons why its disclosure would compromise national security in its classified filings. Plaintiffs no doubt are frustrated that the Court is precluded from giving any more specifics. But "[a]n inherent feature of the state secrets privilege . . . is that the party against whom it is asserted will often not be privy to the information that the Executive seeks to protect." *El-Masri*, 479 F.3d at 312. While the Government must persuade the Court with "[s]ufficient detail" that their assertion of the privilege is warranted, *Al-Haramain*, 507 F.3d at 1203, it has no obligation to divulge any details of the privileged matter to Plaintiffs. (*See* Pls. Opp'n to Gov't, at 31 n.17 (criticizing the Government's public declarations for not describing the alleged privileged information with sufficient specificity). Nevertheless, Plaintiffs' unfamiliarity with the classified materials' explanation for the privilege does not imply that "no such explanation was required," or that the Court's "ruling was simply an unthinking ratification of a conclusory demand by the executive branch." *El-Masri*, 479 F.3d at 312.

C. Consequences of the Privilege Claim

If the court sustains a claim of privilege, then "'the ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim.'" *Jeppesen Dataplan*, 614 F.3d at 1080, 1082 (quoting *Al-Haramain*, 507 F.3d at 1202). Ordinarily, a successful claim of the privilege may simply entail excluding or walling off the secret evidence. *Id.* at 1082. But in some instances, as here, application of the privilege may require dismissal of the case. *Id.* at 1083. Dismissal is appropriate in cases where "the court may be able to de-

termine with certainty from the nature of the allegations and the other government's declarations in support of its claim of secrecy that litigation must be limited or cut off in order to protect state secrets, even before any discovery or evidentiary requests have been made." *Id.* at 1081. There are three circumstances when the *Reynolds* privilege warrants terminating a case entirely, rather than removing the evidence at issue: (1) "if the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence," (2) "if the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant," and (3) "even if the claims and defenses might theoretically be established without relying on privileged evidence, it may be impossible to proceed with the litigation because —privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses—litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Id.* (citations and quotes omitted). The second and third circumstances are applicable here.

1. Privileged Information Needed for Defense

Dismissal of all of Plaintiffs' claims, aside from their FISA claim, is required because the privileged information gives Defendants a valid defense. *Jeppesen Dataplan,* 614 F.3d at 1083. This analysis of the *Reynolds* privilege necessarily coincides with the *Totten* bar, which permits dismissal of an action at the outset if the very subject matter of the action is a state secret. *Reynolds,* 345 U.S. at 11 n.26. The key test is not whether the general subject matter of Operation Flex is a state secret, but whether this case can be "*litigated* without

threatening the disclosure of such state secrets." *El-Masri*, 479 F.3d at 308. "Subject matter" of an action means "those facts that are essential to prosecuting the action or *defending* against it." *Id.* (emphasis added); *see also id.* at 309-11 (affirming dismissal of action under the *Reynolds* privilege because defendants needed privileged information related to CIA intelligence operations to defend itself against plaintiff's claims); *Kasza*, 133 F.3d at 1166 (stating that dismissal is proper "if the privilege deprives the *defendant* of information that would otherwise give the defendant a valid defense to the claim" (citation and quotes omitted)).

Here, Plaintiffs' claims are predicated on their core allegation that Defendants engaged in an indiscriminate investigation, surveillance, and collection of information of Plaintiffs and the putative class because they are Muslim. (FAC ¶¶ 1-3, 86, 167.) Based on this allegation, Plaintiffs assert that Defendants' scheme discriminated against Plaintiffs because of their religion in violation of the Establishment Clause (claims 1, 2); substantially burdened the exercise of their religion without a legitimate government interest in violation of the Free Exercise Clause (claims 3, 4) and the RFRA (claim 5); and violates the Equal Protection Clause (claims 6, 7). Plaintiffs also assert that Defendants' alleged scheme violates the Privacy Act, the Fourth Amendment prohibition against unreasonable searches, and FISA (claims 8, 9, 10). Finally, Plaintiffs assert that the United States is liable to Plaintiffs for the Agent Defendants' invasion of their privacy, violation of Cal. Civ. Code § 52.1, and for intentional infliction of emotional distress under California law pursuant to the FTCA (claim 11).

Plaintiffs contend that they do not need privileged information to prove their discrimination claims against Defendants. (Pls. Opp'n to Gov't, at 37.) The Court does not speculate on what Plaintiffs already have in their possession and whether that is enough to prove their claims at this stage of the proceeding. But even assuming that Plaintiffs do not require privileged information to establish their claims, the Court is persuaded that privileged information provides essential evidence for Defendants' full and effective *defense* against Plaintiffs' claims—namely, showing that Defendants' purported "dragnet" investigations were not indiscriminate schemes to target Muslims, but were properly predicated and focused. Doing so would require Defendants to summon privileged evidence related to Operation Flex, including the subjects who may or may not have been under investigation, the reasons and results of those investigations, and their methods and sources. Additionally, even if Plaintiffs can successfully show that Defendants' actions substantially burdened their exercise of religion with nonprivileged information, defense against Plaintiffs' First Amendment claims entails analysis of whether the Government had a "compelling state interest" and its actions were "narrowly tailored" to achieve that interest. *Church of the Lukumi Babalu Aye, Inc. v. City of Hialeah*, 508 U.S. 520, 546 (1993); *see also Navajo Nation v. United States Forest Serv.*, 535 F.3d 1058, 1068 (9th Cir. 2008) ("[S]hould the plaintiff establish a substantial burden on his exercise of religion [for a RFRA claim], the burden of persuasion shifts to the government to prove that the challenged government action is in furtherance of a 'compelling governmental interest' and is implemented by 'the least restrictive means.'"). These are fact-intensive questions that

necessitate a detailed inquiry into the nature, scope, and reasons for the investigations under Operation Flex. Moreover, with regard to Plaintiffs' FTCA claim, the United States may have a valid defense under the discretionary function exception, *Sabow v. United States,* 93 F.3d 1445, 1451 (9th Cir. 1996), which requires the Court to determine "whether the challenged acts . . . are of the nature and quality that Congress intended to shield from tort liability." *United States v. Varig Airlines,* 467 U.S. 797, 813 (1984); *see also Dichter-Mad Family Partners, LLP v. United States,* 707 F. Supp. 2d 1016, 1018-19 (C.D. Cal. 2010). To establish that this defense applies to the Government's counterterrorism investigations that purportedly violated Plaintiffs' constitutional rights, the Government must marshal facts that fall within the three privileged categories of information related to Operation Flex.[11]

---

[11] Plaintiffs further argue that the Government misunderstands the nature of their religious discrimination claim, which they assert does not require proof that religion is the "sole" reason for their having been targeted for surveillance, but rather that religion was "a" reason that they were targeted. Plaintiffs argue that their essential claim is that religion should be treated like race for the purposes of anti-discrimination law in that its use should always be justified by strict scrutiny. (Pls. Opp'n to Gov't, at 21.) As a preliminary matter, Plaintiffs' characterization of their own allegation contradicts the express language in their FAC. (*See* FAC ¶ 86 (alleging that the FBI Agents' instructions to Monteilh ensured that "Plaintiffs and numerous other people were surveilled *solely* due to their religion") (emphasis added)).) Regardless of the semantics used, however, for the purpose of the state secrets analysis, there is little difference between alleging that Plaintiffs were targeted because of their religion or solely based on their religion. Defense against the claim that Defendants targeted Plaintiffs because of their religion requires the Government to draw on privileged information to show that the in-

2. Inseparable from Privileged Information

Dismissal of Plaintiffs' claims is also required because, even if the claim or defense may be theoretically established without relying on privileged information, the Court is convinced that the privileged and nonprivileged information are inextricably intertwined, such that litigating the instant case to judgment on the merits would present an unacceptable risk of disclosing state secrets. *Jeppesen Dataplan*, 614 F.3d at 1083. "'[W]henever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.'" *Kasza*, 133 F.3d at 1166 (quoting *Ellsberg*, 709 F.2d at 57). But "when, as a practical matter, secret and nonsecret information cannot be separated," the Court may "restrict the parties' access not only to evidence which itself risks the disclosure of a state secret, but also those pieces of evidence or areas of questioning which press so closely upon highly sensitive material that they create a high risk of inadvertent or indirect disclosures." *Jeppesen Dataplan*, 614 F.3d at 1082 (citation and quotes omitted); *see also Kasza*, 133 F.3d at 1166 ("[I]f seemingly innocuous information is part of a classified mosaic, the state secrets privilege may be invoked to bar its disclosure and the court cannot order the government to disentangle this information from other classified information."); *id.* at 1169-70 (affirming dismissal under the state secrets privilege of action involving allegations that the United States Air Force had unlawfully handled hazardous waste in classified operating locations because litigation of plaintiff's claims re-

---

vestigations were proper and narrowly targeted for a legitimate purpose.

quired and risked, under the "classified mosaic" theory, disclosure of privileged information).

Here, as in *Jeppesen Dataplan* and *Kasza*, the subject matter of this case, Operation Flex, involves both privileged and nonprivileged information, which cannot be separated as a practical matter. Indeed, Operation Flex comprises only a small part of the classified mosaic in the FBI's larger counterterrorism investigations, which predate and go beyond Monteilh's source work. The effort to separate privileged from nonprivileged information—even with the protective procedures available to the Court—presents an unjustifiable risk of disclosing state secrets. As the Ninth Circuit observed, "[a]dversarial litigation, including pretrial discovery of documents and witnesses and the presentation of documents and testimony at trial, is inherently complex and unpredictable." *Jeppesen Dataplan*, 614 F.3d at 1089. "Although district courts are well equipped to wall off isolated secrets from disclosure, the challenge is exponentially greater in exceptional cases like this one, where the relevant secrets are difficult or impossible to isolate and even efforts to define a boundary between privileged and unprivileged evidence would risk disclosure by implication." *Id.* In such rare circumstances, as here, the risk of disclosure that further litigation would engender cannot be averted through protective orders or restrictions on testimony. *Id.* This is true even as to Plaintiffs' Fourth Amendment claim because it is impossible to excise the facts directly related to this claim from the factual context of Operation Flex as a whole, and that context forms an important background for a finder of fact to consider in her analysis. While this case is only at the pleading stage and Plaintiffs have not yet propounded any discovery requests, (Arulanantham

Decl. ¶ 2), Defendants need not wait before discovery or evidentiary disputes are at issue to assert the privilege for dismissal. *Jeppesen Dataplan*, 614 F.3d at 1081 ("Courts are not required to play with fire and chance further disclosure—inadvertent, mistaken, or even intentional—that would defeat the very purpose for which the privilege exists.") (quoting *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005)). Accordingly, because further litigation of this action would create "an unjustifiable risk of revealing state secrets" related to the FBI's counterterrorism investigations, dismissal of Plaintiffs' claims is warranted. *Id.* at 614 F.3d at 1088.

V. CONCLUSION

The state secrets privilege strives to achieve a difficult compromise between the principles of national security and constitutional freedoms. The state secrets privilege can only be invoked and applied with restraint, in narrow circumstances, and infused with judicial skepticism. Yet, when properly invoked, it is absolute—the interest of protecting state secrets cannot give way to any other need or interest. Navigating through the narrow straits of the state secrets privilege has not been an easy or enviable task for the Court. In the context of the Executive's counterterrorism efforts engendered by 9/11, the Court has been confronted with the difficult task of balancing its obligation to defer to the Executive in matters of national security with its duty to promote open judicial inquiry. Too much deference would short-circuit constitutional liberties while too much judicial inquiry would risk disclosure of information that would jeopardize national security. In struggling with this conflict, the Court is reminded of the classic dilemma of Odysseus, who faced the challenge of navigating his ship

through a dangerous passage, flanked by a voracious six-headed monster, on the one side, and a deadly whirlpool, on the other. Odysseus opted to pass by the monster and risk a few of his individual sailors, rather than hazard the loss of his entire ship to the sucking whirlpool. Similarly, the proper application of the state secrets privilege may unfortunately mean the sacrifice of individual liberties for the sake of national security. *El-Masri,* 479 F.3d at 313 ("[A] plaintiff suffers this reversal not through any fault of his own, but because his personal interest in pursuing his civil claim is subordinated to the collective interest in national security."); *Sterling,* 416 F.3d at 348 ("[T]here can be no doubt that, in limited circumstances . . . the fundamental principle of access to court must bow to the fact that a nation without sound intelligence is a nation at risk."); *Fitzgerald v. Penthouse Int'l, Ltd.,* 776 F.2d 1236, 1238 n.3 (4th Cir. 1985) ("When the state secrets privilege is validly asserted, the result is unfairness to individual litigants —through the loss of important evidence or dismissal of a case—in order to protect a greater public value.")

The Court recognizes the weight of its conclusion that Plaintiffs must be denied a judicial forum for their claims. The Court does not reach its decision today lightly, but does so only reluctantly, after months of careful review of the parties' submissions and arguments, particularly the Government's *in camera* materials upon which the Court heavily relies. Plaintiffs raise the specter of *Korematsu v. United States,* 323 U.S. 214 (1944), and protest that dismissing their claims based upon the state secrets privilege would permit a "remarkable assertion of power" by the Executive, and that any practice, no matter how abusive, may be immunized from legal challenge by being labeled as "counterterror-

ism" and "state secrets." (Pls. Opp'n to Gov't, at 20, 41-42.) But such a claim assumes that courts simply rubber stamp the Executive's assertion of the state secrets privilege. That is not the case here. The Court has engaged in rigorous judicial scrutiny of the Government's assertion of privilege and thoroughly reviewed the public and classified filings with a skeptical eye. The Court firmly believes that after careful examination of all the parties' submissions, the present action falls squarely within the narrow class of cases that require dismissal of claims at the outset of the proceeding on state secret grounds. Accordingly, all of Plaintiffs' causes of action against Defendants, aside from their FISA claim, are DISMISSED.

APPENDIX D

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 12-56867
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLEES

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; PAT ROSE;
KEVIN ARMSTRONG; PAUL ALLEN, DEFENDANTS

AND

BARBARA WALLS; J. STEPHEN TIDWELL,
DEFENDANTS-APPELLANTS

No. 12-56874
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLEES

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN

TIDWELL, BARBARA WALLS, DEFENDANTS
AND
PAT ROSE; KEVIN ARMSTRONG; PAUL ALLEN,
DEFENDANTS-APPELLANTS

No. 13-55017
D.C. No. 8:11-cv-00301-CJC-VBK

YASSIR FAZAGA; ALI UDDIN MALIK;
YASSER ABDELRAHIM, PLAINTIFFS-APPELLANTS

v.

FEDERAL BUREAU OF INVESTIGATION;
CHRISTOPHER A. WRAY, DIRECTOR OF THE FEDERAL
BUREAU INVESTIGATION, IN HIS OFFICIAL CAPACITY;
PAUL DELACOURT, ASSISTANT DIRECTOR IN CHARGE,
FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES
DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN
TIDWELL; BARBARA WALLS; PAT ROSE; KEVIN
ARMSTRONG; PAUL ALLEN; UNITED STATES OF
AMERICA, DEFENDANTS-APPELLEES

Filed: May 14, 2025

ORDER

Before: GOULD and BERZON, Circuit Judges.[1]

Judge Gould has voted to deny the petition for rehearing en banc and Judge Berzon recommends denial.

---

[1] Judge Steeh has retired. Judge Gould and Judge Berzon are in agreement and decide this matter as a quorum. *See* General Order 3.2(h); 28 U.S.C. § 46(d).

The full court has been advised of the petition and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 40. The petition for rehearing en banc is rejected.

APPENDIX E

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SANTA ANA DIVISION

Case No. SA11-CV-00301 CJC (VBKx)

YASSIR FAZAGA ET AL., PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION ET AL., DEFENDANTS

Filed: Aug. 1, 2011

DECLARATION OF ERIC H. HOLDER
ATTORNEY GENERAL OF THE UNITED STATES

I, Eric H. Holder, hereby state and declare as follows:

1. I am the Attorney General of the United States and head of the United States Department of Justice ('DOJ'), an Executive Department of the United States. *See* 28 U.S.C. §§ 501, 503, 509. The purpose of this declaration is to assert, at the request of the Director of the Federal Bureau of Investigation ("FBI"), and in my capacity as Attorney General and head of DOJ, a formal claim of the state secrets privilege in order to protect the national security interests of the United States. The statements made herein are based on my personal know-

ledge, on information provided to me in my official capacity, and on my evaluation of that information.

2. In the course of my official duties, I have been informed that the plaintiffs in this action—three Muslim residents of southern California—have filed a class action against the FBI, FBI Director Robert Mueller and Steven M. Martinez, Assistant Director in Charge of the FBI's Los Angeles Field Office, in their official capacities, claiming alleged violations of the Free Exercise Clause and Establishment Clause of the First Amendment, the Religious Freedom Restoration Act, the equal protection principles of the Fifth Amendment, the Privacy Act, the Fourth Amendment, and the Foreign Intelligence Surveillance Act, and for conspiracy to violate the plaintiff's civil rights pursuant to 42 U.S.C. § 1985(3). I understand that the plaintiffs allege that the defendants, through the use of a paid confidential informant, engaged in an impermissible investigation to collect personal information indiscriminately on the plaintiffs and others based solely on their religion in violation of their rights under the Constitution and statutory law.

3. I have read and carefully considered the public and classified declarations of Mark Giuliano ("Giuliano Declaration"), Assistant Director of the FBI's Counterterrorism Division. After careful and actual personal consideration of the matter, I have concluded that disclosure of the three categories of information described below and in more detail in the classified Giuliano Declaration could reasonably be expected to cause significant harm to the national security, and I therefore formally assert the state secrets privilege over this information. The classified Giuliano Declaration, which is available for the Court's *ex parte, in camera* review, de-

scribes in classified detail the information over which I am asserting the state secrets privilege. As Attorney General, I possess original classification authority under § 1.3 of Executive Order ("E.O.") 13526, dated December 29, 2009. *See* 75 Fed. Reg. 707. The classified Giuliano Declaration is properly classified under § 1.2 E.O. 13526 because public disclosure of the information contained in that declaration also could reasonably be expected to cause significant harm to national security.

4. In unclassified terms, my privilege assertion encompasses information in the following categories:

(i) *Subject Identification*: Information that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation, including in Operation Flex.

(ii) *Reasons for Counterterrorism Investigations and Results*: Information that could tend to reveal the initial reasons (*i.e.*, predicate) for an FBI counterterrorism investigation of a particular person (including in Operation Flex), any information obtained during the course of such an investigation, and the status and results of the investigation. This category includes any information obtained from the U.S. Intelligence Community related to the reasons for an investigation.

(iii) *Sources and Methods*: Information that could tend to reveal whether particular sources and methods were used in a counterterrorism investigation of a particular subject, including in Operation Flex. This category includes previously undisclosed information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative sources and methods were used in a counterterrorism investigation of a particular person, the reasons such methods

were used, the status of the use of such sources and the methods, and any results derived from such methods.

5. As indicated above and explained further below, I have determined that disclosure of information falling into the foregoing categories could reasonably be expected to cause significant harm to national security.

6. First, I concur with the FBI's determination that the disclosure of the identities of subjects of counterterrorism investigations, including Operation Flex, reasonably could be expected to cause significant harm to national security. As the FBI has explained, such disclosures would alert those subjects to the FBI's interest in them and cause them to attempt to flee, destroy evidence, or alter their conduct so as to avoid detection of their future activities, which would seriously impede law enforcement and intelligence officers' ability to determine their whereabouts or gain further intelligence on their activities. In addition, as the FBI has explained, knowledge that they were under investigation could enable subjects to anticipate the actions of law enforcement and intelligence officers, possibly leading to countersurveillance that could place federal agents at higher risk, and to ascertain the identities of confidential informants or other intelligence sources, placing those sources at risk. Such knowledge, as the FBI has further explained, could also alert associates of the subjects to the fact that the FBI is likely aware of their associations with the subjects and cause them to take similar steps to avoid scrutiny.

7. Second, I agree with the FBI that disclosure that an individual is not a subject of a national security investigation could likewise reasonably be expected to cause significant harm to national security. As the FBI

has explained, disclosure that some persons are not subject to investigation, while the status of others is left unconfirmed, would inherently reveal that FBI concerns remain as to particular persons. Allowing such disclosures, as the FBI indicates, would enable individuals and terrorist groups alike to manipulate the system to discover whether they or their members are subject to investigation. Further, as the FBI has pointed out, individuals who desire to commit terrorist acts could be motivated to do so upon discovering that they are not being monitored.

8. In addition, I agree with the FBI's judgment that where an investigation of a subject has been closed, disclosure that an individual was formerly the subject of a counterterrorism investigation could also reasonably be expected to cause significant harm to national security. Again, I agree with the FBI that, to the extent that an individual had terrorist intentions that were not previously detected, the knowledge that he or she is no longer the subject of investigative interest could embolden him or her to carry out those intentions. Moreover, as the FBI indicates, the fact that investigations are closed does not mean that the subjects have necessarily been cleared of wrongdoing, as closed cases are often reopened based on new information. As the FBI has also explained, even if the former subjects are law-abiding, the disclosure that they had been investigated could still provide valuable information to terrorists and terrorist organizations about the FBI's intelligence and concerns, particularly where the former subjects have associates whom the FBI may still be investigating based on the FBI's interest in the closed subject could alert such associates to the FBI's interest in them and lead them to

destroy evidence or alter their conduct so as to avoid detection of their future activities.

9. Third, I agree with the FBI's judgment that disclosure of the reasons for and substance of a counterterrorism investigation—whether the initial predicate for opening an investigation, information gained during the investigation, or the status or results of the investigation —could also reasonably be expected to cause significant harm to national security. As the FBI has determined, such disclosures would reveal to subjects who are involved in or planning to undertake terrorist activities what the FBI knows or does not know about their plans and the threat they pose to national security. Even if the subjects have no terrorist intentions, as the FBI has explained, disclosure of the reasons they came under investigation may reveal sensitive intelligence information about them, their associates, or particular threat that would harm other investigations. More generally, as the FBI has also explained, disclosure of the reasons for an investigation could provide insights to persons intent on committing terrorist attacks as to what type of information is sufficient to trigger an inquiry by the FBI, and what sources and methods the FBI employs to obtain information on a person.

10. Finally, I agree with the FBI that the disclosure of certain information that would tend to describe, reveal, confirm or deny the existence or use of FBI investigative sources and methods, or techniques used in the counterterrorism investigations at issue in this case could likewise be reasonably expected to cause significant harm to national security. This aspect of my privilege assertion would include information that would tend to reveal whether court-ordered searches or sur-

veillance, confidential human sources, and other investigative sources and methods were used in a counterterrorism investigation of a particular person, the reasons for and the status of the use of such sources and methods, and any results derived from such methods. The disclosure of such information, as the FBI has explained, could reveal not only the identities of particular subjects but also the steps taken by the FBI in counterterrorism matters. I agree with the FBI's assessment that such information would effectively provide a road map to adversaries on how the FBI goes about detecting and preventing terrorist attacks.

11. Any further elaboration concerning the foregoing matters on the public record would reveal information that could cause the very harms my assertion of the state secrets privilege is intended to prevent. The classified Giuliano Declaration, submitted for *ex parte, in camera*, provides a more detailed explanation of the information over which I am asserting the privilege and the harms to national security that would result from disclosure of that information.

12. On September 23, 2009, I announced a new Executive Branch policy governing the assertion and defense of the state secrets privilege in litigation. Under the policy, the Department of Justice will defend an assertion of the state secrets privilege in litigation, and seek dismissal of a claim on that basis, only when "necessary to protect against the risk of significant harm to national security." *See* Exhibit 1 (State Secrets Policy) ¶ 1(A). The policy provides further that an application of a privilege assertion must be narrowly tailored and that dismissal be sought pursuant to the privilege assertion only when necessary to prevent significant harm to

national security. *Id.* ¶ 1(B). Moreover, "[t]he Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States government; (iii) restrain competition; or (iv) prevent or delay the release of information the release of which would not reasonably be expected to cause significant harm to national security." *Id.* ¶ 1(C). The policy also established detailed procedures for review of a proposed assertion of the state secrets privilege in a particular case. *Id.* ¶ 2. Those procedures require submissions by the relevant government departments or agencies specifying "(i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; [and] (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm." *Id.* ¶ 2(A). Based on my personal consideration of the matter, I have determined that the requirements for an assertion and defense of the state secrets privilege have been met in this case in accord with the September 2009 State Secrets Policy.

I declare under penalty of perjury that the foregoing is true and correct

Executed this [29th] day of July, 2011, in Washington, D.C.

/s/ ERIC H. HOLDER
ERIC H. HOLDER
Attorney General of the United States

EXHIBIT 1 TO DECLARATION OF ATTORNEY GENERAL ERIC H. HOLDER

Office of the Attorney General

Washington, D.C. 20530

Sept. 23, 2009

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

MEMORANDUM FOR THE HEADS OF DEPARTMENT COMPONENTS

FROM: [EH] THE ATTORNEY GENERAL

SUBJECT: Policies and Procedures Governing Invocation of the State Secrets Privilege

I am issuing today new Department of Justice policies and administrative procedures that will provide greater accountability and reliability in the invocation of the state secrets privilege in litigation. The Department is adopting these policies and procedures to strengthen public confidence that the U.S. Government will invoke privilege in court only when genuine and significant harm to national defense or foreign relations is at stake and only to the extent necessary to safeguard those interests. The policies and procedures set forth in this Memorandum are effective as of October 1, 2009, and the Department shall apply them in all cases in which a government department or agency thereafter seeks to invoke the state secrets privilege in litigation.

1. Standards for Determination

A. Legal Standard. The Department will defend an assertion of the state secrets privilege ('privilege") in litigation when a government department or agency

seeking to assert the privilege makes a sufficient showing that assertion of the privilege is necessary to protect information the unauthorized disclosure of which reasonably could be expected to cause significant harm to the national defense or foreign relations ('national security") of the United States. With respect to classified information, the Department will defend invocation of the privilege to protect information properly classified pursuant to Executive Order 12958, as amended, or any successor order, at any level of classification, so long as the unauthorized disclosure of such information reasonably could be expected to cause significant harm to the national security of the United States. With respect to information that is nonpublic but not classified, the Department will also defend invocation of the privilege so long as the disclosure of such information reasonably could be expected to cause significant harm to the national security of the United States.

B. Narrow Tailoring. The Department's policy is that the privilege should be invoked only to the extent necessary to protect against the risk of significant harm to national security. The Department will seek to dismiss a litigant's claim or case on the basis of the state secrets privilege only when doing so is necessary to protect against the risk of significant harm to national security.

C. Limitations. The Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States government; (iii) restrain competition; or (iv) prevent or delay the re-

lease of information the release of which would not reasonably be expected to cause significant harm to national security.

2. Initial Procedures for Invocation of the Privilege

A. Evidentiary Support. A government department or agency seeking invocation of the privilege in litigation must submit to the Division in the Department with responsibility for the litigation in question[1] a detailed declaration based on personal knowledge that specifies in detail: (i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm; and (iv) any other information relevant to the decision whether the privilege should be invoked in litigation.

B. Recommendation from the Assistant Attorney General. The Assistant Attorney General for the Division responsible for the matter shall formally recommend in writing whether or not the Department should defend the assertion of the privilege in litiga-

[1] The question whether to invoke the privilege typically arises in civil litigation. Requests for invocation of the privilege in those cases shall be addressed to the Civil Division. The question whether to invoke the privilege also may arise in cases handled by the Environment and Natural Resources Division (ENRD), and requests for invocation of the privilege shall addressed to ENRD in those instances. It is also possible that a court may require the Government to satisfy the standards for invoking the privilege in criminal proceedings. *See United States v. Araf*, 533 F.3d 72, 78-80 (2d Cir. 2008); *but see United States v. Rosen*, 557 F.3d 192,198 (4th Cir. 2009). In such instances, requests to submit filings to satisfy the standard shall be directed to the National Security Division.

tion. In order to make a formal recommendation to defend the assertion of the privilege, the Assistant Attorney General must conclude, based on a personal evaluation of the evidence submitted by the department or agency seeking invocation of the privilege, that the standards set forth in Section 1(a) of this Memorandum are satisfied. The recommendation of the Assistant Attorney General shall be made in a timely manner to ensure that the State Secrets Review Committee has adequate time to give meaningful consideration to the recommendation.

3. State Secrets Review Committee

A. Review Committee. A State Secrets Review Committee consisting of senior Department of Justice officials designated by the Attorney General will evaluate the Assistant Attorney General's recommendation to determine whether invocation of the privilege in litigation is warranted.

B. Consultation. The Review Committee will consult as necessary and appropriate with the department or agency seeking invocation of the privilege in litigation and with the Office of the Director of National Intelligence. The Review Committee must engage in such consultation prior to making any recommendation against defending the invocation of the privilege in litigation.

C. Recommendation by the Review Committee. The Review Committee shall make a recommendation to the Deputy Attorney General, who shall in turn make a recommendation to the Attorney General.[2] The rec-

[2] In civil cases, the review committee's recommendation should be made through the Associate Attorney General to the Deputy Attor-

ommendations shall be made in a timely manner to ensure that the Attorney General has adequate time to give meaningful consideration to such recommendations.

4. **Attorney General Approval**

A. Attorney General Approval. The Department will not defend an assertion of the privilege in litigation without the personal approval of the Attorney General (or, in the absence or recusal of the Attorney General, the Deputy Attorney General or the Acting Attorney General).

B. Notification to Agency or Department Head. In the event that the Attorney General does not approve invocation of the privilege in litigation with respect to some or all of the information a requesting department or agency seeks to protect, the Department will provide prompt notice to the head of the requesting department or agency.

C. Referral to Agency or Department Inspector General. If the Attorney General concludes that it would be proper to defend invocation of the privilege in a case, and that invocation of the privilege would preclude adjudication of particular claims, but that the case raises credible allegations of government wrongdoing, the Department will refer those allegations to the Inspector General of the appropriate department or agency for further investigation, and will provide prompt notice of the referral to the head of the appropriate department or agency.

---

ney General, who shall in turn make a recommendation to the Attorney General.

5. Reporting to Congress

The Department will provide periodic reports to appropriate oversight committees of Congress with respect to all cases in which the Department invokes the privilege on behalf of departments or agencies in litigation, explaining the basis for invoking the privilege.

6. Classification Authority

The department or agency with classification authority over information potentially subject to an invocation of the privilege at all times retains its classification authority under Executive Order 12958, as amended, or any successor order.

7. No Substantive or Procedural Rights Created

This policy statement is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

APPENDIX F

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SANTA ANA DIVISION

Case No. SACV11-00301 CJC (VBKx)

YASSER FAZAGA, ET AL., PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATIONS, ET AL., DEFENDANTS

Filed: Aug. 1, 2011

PUBLIC DECLARATION OF MARK F. GIULIANO
FEDERAL BUREAU OF INVESTIGATION

I, Mark F. Giuliano, hereby declare the following:

1. I am the Assistant Director, Counterterrorism Division, Federal Bureau of Investigation (the FBI), United States Department of Justice. I am responsible for, among other things, directing the conduct of FBI counterterrorism investigations. As Assistant Director, I have official supervision and control over the files and records of the Counterterrorism Division, FBI Headquarters, Washington, D.C. In addition, I have been delegated original classification authority by the Director of the FBI. *See* Executive Order 13,526, Section 1.3(c). As a result, and pursuant to all applicable Executive Orders, I am responsible for the protection of clas-

sified national security information within the Counterterrorism Division of the FBI, including the sources and methods used by the FBI in the collection of national security information. I have been authorized by the Director of the FBI to execute declarations and affidavits in order to protect such information. The matters stated herein are based on my personal knowledge and on information furnished to me in the course of my official duties.

2. I submit this declaration in support of the Attorney General's assertion of the state secrets privilege in this case. I describe below, as best I am able to do in unclassified terms, certain information related to FBI counterterrorism investigations that is implicated by the allegations of this lawsuit and which in my judgment should be protected from disclosure to avoid significant harm to national security.[1] As an original FBI classification authority and the official charged with general supervisory responsibilities for the FBI's counterterrorism investigations, I have concluded that the unauthorized disclosure of the privileged information described herein reasonably could be expected to cause significant harm to the national security.

SUMMARY

3. I have reviewed the Complaint in this matter and I am aware of the allegations it contains that the FBI, through Craig Monteilh acting as an informant for the FBI in an investigation known as Operation Flex, infiltrated mosques in Southern California and indiscrimi-

[1] I am also separately providing a declaration solely for the Court's *ex parte, in camera* review, that discusses these matters in more detail with reference to information that cannot be disclosed on the public record.

nately collected personal information on hundreds and perhaps thousands of innocent Muslim Americans, including the three named plaintiffs, Yassir Fazaga, Ali Uddin Malik and Yasser AbdelRahim, due solely to their religion. *See* Complaint, ¶¶ 1-3, 6, 84. The plaintiffs specifically allege that, after attacks of September 11, 2001, the FBI has improperly focused its counterterrorism efforts on the Muslim community in the United States. *See id.* ¶¶ 24-27. The plaintiffs also cite guidelines issued by the Attorney General for counterterrorism investigations and assert that "the combined effect" of these guidelines was to authorize the FBI to engage in intrusive investigation of First Amendment protected activity, and specifically religious practices, without any factual basis to believe any criminal violations or threat to national security existed. *See* Compl. ¶¶ 28-35. Plaintiffs also allege that guidelines issued by the Attorney General in 2008, as well as the FBI's *Domestic Intelligence and Operations Guides (*"DIOG"*)* published in December 2008, permit investigative activity "based on extremely limited information, including information about the First Amendment expression of subjects." *See* Compl. ¶¶ 36-37. Accordingly, this lawsuit puts at issue whether the FBI has undertaken counterterrorism investigative activity of Muslim Americans and mosques in Southern California, and of the three plaintiffs in particular, through the use of Monteilh as an informant, which was impermissibly based solely on religion or First Amendment-protected activities.

4. The Attorney General Guidelines and FBI policies cited by the plaintiffs in the Complaint include a prohibition on the FBI's undertaking investigative activity based solely on First Amendment activities. For example, *The Attorney General's Guidelines for FBI*

National Security Investigations and Foreign Intelligence Collection, effective October 31, 2003 (Excerpts at Tab 1) ("AG 2003"), and the Guidelines which superseded them, *The Attorney General's Guidelines for Domestic FBI Operations* issued by the Attorney General on September 29, 2008 (Excerpts at Tab 2) ("AG 2008"), state: "These guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States." *See* Tab 2, AG 2008 at 13; *see also* Tab 1, AG 2003 at 7-8.

5. Likewise, the FBI's DIOG contains an extensive discussion of the FBI's policy to undertake its investigations with full adherence to the Constitutional protections and civil liberties of the American people. *See* Tab 3 (DIOG Excerpts). In particular, the DIOG prohibits investigative activity conducted for the sole purpose of monitoring the exercise of Constitutional rights or on the basis of race, ethnicity, national origin, or religion. *See* DIOG at 21-38. Under the DIOG, there must be an authorized purpose for investigative activity that could have an impact on religious practice. *Id.* at 21. The DIOG provides that an authorized purpose of FBI investigative activity must avoid actual—and the appearance of—interference with religious practice to the maximum extent possible. *Id.* at 27. The DIOG also explains, however, that this policy does not mean that religious practitioners or religious facilities are completely free from being examined as part of FBI investigative activity. If such practitioners are involved in —or such facilities are used for—activities that are the proper subject of FBI-authorized investigative or intelligence collection activi-

ties, religious affiliation does not immunize them to any degree from FBI investigative action. *Id.* Nonetheless, FBI policy states that the authorized purpose of an investigation must be properly documented and that investigative activity directed at religious leaders or occurring at religious facilities must be focused in time and manner so as not to infringe on legitimate religious practice by any individual but especially by those who appear unconnected to the activities under investigation. *Id.*

6. Addressing plaintiffs' allegations in this case will risk or require the disclosure of certain sensitive information concerning counterterrorism investigative activity in Southern California, including in particular the nature and scope of Operation Flex. As indicated below, the FBI previously has acknowledged that it utilized Mr. Monteilh as a confidential human source and has disclosed some limited information concerning his actions. However, certain specific information pertinent to the allegations about Operation Flex and Monteilh's activities remains highly sensitive information concerning counterterrorism matters that if disclosed reasonably could be expected to cause significant harm to national security. As described below, this includes:

(i) the identities of individuals who have or have not been the subject of counterterrorism investigations, including in Operation Flex, and the status and results of any such investigations;

(ii) information concerning why particular individuals were subject to investigation, including in Operation Flex; and

(iii) particular sources and methods used in obtaining information for counterterrorism investigations, including in Operation Flex.

BACKGROUND

A. The Continuing Terrorist Threat Since September 11, 2001

7. Before describing the information that the FBI seeks to protect in this case through the Attorney General's privilege assertion, I set forth some background on the FBI's counterterrorism actions since the 9/11 attacks. FBI Director Robert Mueller has made clear that the FBI's number one priority continues to be the prevention of terrorist attacks against the United States.[2] As Director Mueller explained in Congressional testimony, since the 2001 terrorist attacks, al Qaeda's intent to conduct high-profile attacks inside the United States has been unwavering. Recent investigations reveal that the group has adapted its strategy for conducting such attacks. In the immediate aftermath of 9/11, al Qaeda's plots and plans primarily focused on using individuals from the Middle East or South Asia for such attacks. More recent plots—beginning in August 2006 with the attempted plan to commit attacks against U.S.-bound aircraft using improvised explosive devices —suggest al Qaeda is also putting more emphasis on finding recruits or trainees from the West to play key roles for these homeland specific operations.

8. Al Qaeda's effort to recruit, train, and deploy operatives to attack worldwide, but specifically in the United States, was demonstrated with the arrest of Najibullah Zazi, who was plotting to attack the New

---

[2] *See* Testimony of Director Mueller before the Senate Committee on Homeland Security and Governmental Affairs (Sept. 22, 2010) (available at http://www.fbi.gov/news/testimony/nine-years-after-9-11-confronting-the-terrorist-threat-to-the-u.s (last visited on July 20, 2011).

York City subway system. The fact that Zazi and his associates had access to the United States and were familiar with the environment here from an operational security and targeting perspective demonstrates how al Qaeda can leverage Americans. The potential exists for al Qaeda to use and train other Americans for additional homeland attacks. Identifying these individuals is among the FBI's highest counterterrorism priorities.

9. A similar example may be seen in the May 2010 failed attempt of Faisal Shazad to detonate a car bomb in Times Square, an attack for which Tehrik-e-Taliban in Pakistan (TTP) claimed responsibility. Like al Qaeda's use of Zazi, TTP's use of Shazad—a naturalized U.S. citizen who had lived for years in the United States—to attempt to attack the homeland underscores the operational role people in the United States can play for al Qaeda and its affiliates. Similarly, al Qaeda of the Arabian Peninsula (AQAP) demonstrated its intent to target the U.S. homeland in the failed attempt by Umar Farouk Abdulmutallab to bomb Northwest Flight 253 to Chicago on December 25, 2009. Much like the other attacks, AQAP was able to identify a willing recruit who was committed to attacking the United States and whose background did not raise traditional security scrutiny.

10. The threat of homegrown violent extremists—those who have lived primarily inside the United States and may commit acts of violence in furtherance of the objectives of a foreign terrorist organization—also remains a particular concern. Such individuals may be inspired by the global jihadist movement to commit violent acts inside the United States but do not necessarily receive direct guidance from terrorist groups overseas. A good example of this type of homegrown threat oc-

curred in the Los Angeles area. On September 11, 2005, a group of armed men planned to enter a military recruiting center on a busy street in Santa Monica and kill everyone inside. Their plan was to then go underground for a month and re-emerge on Yom Kippur. They plotted to open fire on families gathered outside a temple in West Los Angeles, preparing to celebrate the holy day. The members of this homegrown cell planned these attacks in a jail cell in Folsom Prison. They had no official connection to al Qaeda, but they had adopted its cause. They had raised the money, recruited the participants, chosen the targets, obtained the weapons, and set the date. These terrorists were poised to strike, but they made a key mistake by first committing a series of gas station robberies to raise money to finance their attacks. Police in Torrance, California, arrested two of the men for robbery and, when their apartment was searched, documents were discovered that listed the addresses of military recruiting stations and local synagogues. The Torrance police then contacted the Los Angeles Joint Terrorism Task Force (JTTF). From that point, hundreds of investigators worked at an FBI command post to identify other members of the cell. Ultimately, the FBI, working through the JTTF, was able to disrupt this particular home grown attack. But the threat of such attacks persists, and the FBI continues to devote extensive effort to detecting and preventing other such attacks.

B. <u>The FBI's Use of Monteilh as Confidential Source</u>

11. In 2009, the FBI acknowledged that it utilized Monteilh as a confidential human source during a criminal proceeding in this district involving Ahmadullah Ni-

azi.[3] From 2006-2007, Monteilh reported on a group of counterterrorism investigations that was given the name Operation Flex. Operation Flex focused on fewer than 25 individuals and was directed at detecting and preventing possible terrorist attacks. The goal of Operation Flex was to determine whether particular individuals were involved in the recruitment and training of individuals in the United States or overseas for possible terrorist activity.

12. The FBI has previously disclosed some of the actions Mr. Monteilh undertook as a confidential informant for the FBI and some of the information he collected for the FBI. Specifically, during the *Niazi* criminal case noted above, the FBI disclosed to the defendant in that case the content of some of the audio and video recordings containing conversations between Mr. Monteilh and the defendant and others. The FBI also acknowledged in the *Niazi* case that Mr. Monteilh provided handwritten notes to the FBI, and it produced certain notes provided by Mr. Monteilh concerning Mr. Niazi. The FBI is presently assessing whether additional audio, video, or notes can be disclosed without risking disclosure of the privileged information described below and significant harm to national security interests in protecting counterterrorism investigations.

---

[3] In the criminal case *United States v. Ahmadullah Niazi*, U.S.D.C., C.D. Cal., No. SACR 09-28-AN, FBI Special Agent Thomas Ropel testified at a detention hearing in that case that an FBI informant who had provided information concerning Mr. Niazi was the same person Mr. Niazi had reported to the FBI as a possible terrorist. Although SA Ropel did not identify Mr. Monteilh by name, Mr. Niazi knew that Monteilh was the person he had reported to the FBI as a possible terrorist. (The *Niazi* indictment in that criminal case was later dismissed by the United States without prejudice.)

13. However, as set forth below, the FBI must protect certain specific information concerning counterterrorism investigative matters related to the allegations of this case, including Operation Flex in which Monteilh was involved. In particular, the FBI cannot publicly disclose the identities of specific subjects of counterterrorism investigations (some of which remain open), the identities of those who have not been subject to investigation, the precise number of Operation Flex subjects, the reasons particular individuals were subject to investigation, or particular sources and methods of investigation used in counterterrorism cases.

14. Monteilh has provided numerous statements to the media discussing his purported activities on behalf of the FBI. He has also filed his own lawsuit against the FBI and agents in their personal capacity in which he makes allegations related to his work as an FBI source. *See Monteilh v. FBI,* et al., U.S.D.C., C.D. Cal., Civil Action No. 10-102. The FBI has not confirmed or denied any of Monteilh's public allegations concerning his work for the FBI, and his allegations do not constitute a disclosure or confirmation by the FBI of any information concerning his activities as an informant.

INFORMATION SUBJECT TO STATE SECRETS PRIVILEGE AND HARM TO NATIONAL SECURITY FROM DISCLOSURE

15. The categories of information that the FBI seeks to protect in this case through the Attorney General's privilege assertion are described below. Upon my personal consideration, I have determined that disclosure of information in these categories reasonably could be expected to cause significant harm to national security:

(1) ***Subject Identification***: Information that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation, including in Operation Flex.

(2) ***Reasons for Counterterrorism Investigations and Results***: Information that could tend to reveal the initial reasons (*i.e.* predicate) for an FBI counterterrorism investigation of a particular person (including in Operation Flex), any information obtained during the course of such an investigation, and the status and results of the investigation. This category includes information obtained from the U.S. Intelligence Community related to the reasons for an investigation.

(3) ***Sources and Methods***: Information that could tend to reveal whether particular sources and methods were used in a counterterrorism investigation of a particular subject, including in Operation Flex. This category includes previously undisclosed information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative sources and methods, were used in a counterterrorism investigation of a particular person, the reasons such methods were used, the status of the use of such sources and methods, and any results derived from such methods.[4]

---

[4] This description of the broad categories of information subject to the Attorney General's claim of privilege is not meant to foreclose the possibility that other information related to FBI counterterrorism investigations including Operation Flex may be identified in later proceedings as subject to privilege.

I. Subject Identification and Reasons for Investigation

16. The FBI seeks to protect through the Attorney General's privilege assertion information that would confirm or deny whether particular individuals were the subjects of FBI counterterrorism investigations, and the predicate for, information obtained in, and the status and results of any counterterrorism investigations action of particular persons. I describe below in unclassified terms why the disclosure of such information reasonably could be expected to cause significant harm to national security. I address first the process for approval and oversight of FBI counterterrorism investigations under then-applicable Attorney General Guidelines.

A. Counterterrorism Guidelines Applicable to Operation Flex

17. At the time the investigations at issue in this case were opened, the October 31, 2003 Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG) were in effect. The NSIG authorized three levels of investigative activity: threat assessments, preliminary investigations and full investigations.

18. The 2003 AG Guidelines authorized the FBI to undertake threat assessments to proactively draw on available sources of information to identify terrorist threats and activities through non-intrusive investigative techniques, including obtaining publicly available information, accessing information available within the FBI and Department of Justice, requesting information from other government entities, using online resources, interviewing previously established assets, and conducting non-pretextual interviews of members of the public

and private entities. The authority to undertake threat assessments could be used in cases in which information or an allegation concerning possible terrorist activity or other national security threats by an individual, group, or organization were received by the FBI and the matter could be checked promptly through the relatively non-intrusive means described above.

19. A Preliminary Investigation could be initiated under the 2003 guidelines to determine whether a full investigation was appropriate based upon "information or an allegation" indicating a threat to the national security, for example, that an individual is or may be an international terrorist or an agent of a foreign power; an individual, group or organization is or may be engaging, or has or may have engaged, in activities constituting a threat to the national security (or related preparatory or support activities) for or on behalf of a foreign power; or an individual, group or organization is, or may be, the target of a recruitment or infiltration effort by an international terrorist, foreign power, or agent of a foreign power under circumstances related to a threat to the national security. Most Preliminary Investigations could be approved by either the Special Agent in Charge (SAC) of the field office or, as authorized by the Special Agent in Charge, by an Assistant Special Agent in Charge (ASAC) or squad supervisor with responsibility for national security investigations. A field office was required under the 2003 guidelines to notify FBI Headquarters of the initiation of the investigation and to identify the grounds for the investigation. FBI Headquarters, in turn, was required to provide notice of the initiation of the investigation to the Department of Justice's

Office of Intelligence Policy and Review (OIPR).[5] All lawful investigative techniques could be used in a Preliminary Investigation except for mail opening, physical search, or electronic surveillance requiring judicial order or warrant.

20. A Preliminary Investigation was to be completed within six months of the date of initiation, but if warranted by facts or information obtained in the course of the investigation, senior field office managers could authorize a six-month extension. An extension of a Preliminary Investigation beyond the initial one-year period required FBI Headquarters approval and could be granted in six-month increments. FBI Headquarters was required to notify OIPR of any extensions by FBI Headquarters beyond the initial one-year period.

21. A Full Investigation was authorized under the same circumstances as a Preliminary Investigation except that instead of "information or an allegation" of a threat to the national security the NSIG required that "specific and articulable facts" gave reason to believe that a threat to the national security may exist. Most Full Investigations could be approved by either the SAC of the field office or, as authorized by the SAC, by an ASAC. The notice requirements for the initiation of a Full Investigation were the same as for the initiation of a Preliminary Investigation. All lawful investigative techniques could be used in a Full Investigation. The FBI was required under the 2003 guidelines to notify OIPR and the Criminal Division at the end of each year a full investigation continued and to provide OIPR and

---

[5] The Office of Intelligence Policy and Review became part of the National Security Division (NSD) in the Department of Justice and has been renamed the Office of Intelligence.

the Criminal Division with a summary of the investigation.

22. All of the investigations of Operation Flex subjects were opened with supervisory authority and subject to internal FBI and DOJ oversight.

B. Harm to National Security from Disclosure of Counterterrorism Investigation Subjects and Reasons for Investigation

23. Disclosure of the identity of subjects of counterterrorism investigations could reasonably be expected to result in significant harm to national security. First, disclosure of the subjects of open counterterrorism investigations would obviously alert those subjects to the fact of the FBI's current interest in them. Such knowledge would cause significant harm to FBI counterterrorism investigations, as subjects could attempt to flee, destroy evidence or take steps to alter their conduct so as to avoid detection of their future activities by law enforcement. In these circumstances, law enforcement and intelligence officers would be significantly hindered in gathering further intelligence on their activities or determine their whereabouts. In addition, knowledge that they were under investigation might enable subjects to anticipate the activities of law enforcement and intelligence officers, perhaps conducting counter-surveillance activities that could place Federal agents at greater risk. Such knowledge would also alert associates of the subjects to the fact that the FBI is likely aware of their associations with the subject, causing them to take similar steps to avoid scrutiny. Disclosing the identities of counterterrorism subjects also could enable subjects to ascertain the identities of confidential informants or other sources of intelligence, putting those sources at risk.

24. Disclosure that an individual is *not* a subject of a national security investigation also reasonably could be expected to cause significant harm to national security. Individuals or terrorist groups could manipulate the system to discover whether they or their members are subject to investigation. Disclosure that some persons are not subject to investigation, while the status of others is not confirmed, would inherently reveal that concerns remains as to particular persons. Also, if individuals desire to commit terrorist acts, notification that they are not under investigation would inform them that they can move without detection. Indeed, confirmation that an individual is not under investigation could provide an incentive to those so inclined to commit a terrorist act before becoming subject to investigative interest.

25. Similarly, even where an investigation has been closed, disclosing that an individual formerly was the subject of a counterterrorism investigation reasonably could be expected to cause significant harm to national security. Disclosure that an individual had been, but is no longer, under investigation might induce that subject to evaluate previous conduct and interactions to determine what information the Government may have obtained about them. As noted, to the extent that the individual's terrorism-related intentions were not previously detected and the individual later decided to undertake terrorist activity, knowing one was no longer the subject of investigative interest might embolden that person to operate confident that there is not a threat of detection. In addition, the fact that investigations are closed typically does not indicate that the subjects have been "cleared" of wrongdoing. Closed cases are often reopened based on new information.

26. Even if individuals are entirely law-abiding, disclosure that they were once, but no longer are, the subjects of counterterrorism investigations would provide valuable intelligence to suspected terrorists and terrorist organizations regarding the intelligence and suspicions the FBI has regarding them. Indeed, even if the FBI has closed an investigation on one subject, it may have open investigations on the associates of that subject who are engaged in or still suspected of ties to terrorist activity. Disclosing that investigations on certain persons are closed where the FBI has not found a current nexus to terrorism could still alert their associates of the FBI interests in *them*, which could lead these associates to destroy evidence or alter their conduct so as to avoid detection of their future activities by law enforcement.

27. In addition, disclosure that a person had been a subject of a closed counterterrorism investigation would also provide an important insight into the FBI's investigative sources and methods. The FBI may open a counterterrorism investigation based on an individual's association with a subject of another open counterterrorism investigation, when the association is close enough to indicate a threat to the national security. If the subjects of FBI investigations were disclosed, individuals closely associated with that subject would be on notice that they may be subjects of investigations, and thus take steps to avoid detection.

28. Even if a person believes that he or she might have been under investigation based on unconfirmed public speculation or other information, confirmation of that fact by the Government in litigation would remove all doubt and would not only confirm who was or was not subject to investigation, but would tend to reveal why

the Government had a particular interest or concern with certain individuals. This would inherently reveal the focus (or lack thereof) of investigative action.

29. Similarly, disclosure of the substance of a counterterrorism investigation—whether the initial predicate, information gained during the investigation, status, and results—would reveal a range of sensitive counterterrorism investigative in formation, even if the investigation does not identify any nexus to terrorism. There is, first, the obvious harm of revealing to subjects who may in fact be bent on terrorist activity what the FBI knows or does not know about their plans and the threat they pose to national security. Even if a person is not intent on committing terrorist acts, the reasons they came under suspicion may involve sensitive intelligence information about them, their associates, or a particular threat, the disclosure of which could harm other pending or future investigations. More generally, disclosure of the reasons for an investigation could indicate what kind of information is sufficient to trigger an inquiry by the FBI, thus providing insights to those intent on terrorism on how to avoid detection. Finally, as discussed further below, disclosure of the reasons for an investigation may reveal sensitive sources and methods related to how the FBI may obtain information on a person.

II. FBI Investigative Sources, Methods, Techniques in Operation Flex

30. The FBI also seeks to protect through the Attorney General's privilege assertion information that would tend to describe, reveal, confirm or deny the existence or use of FBI investigative sources, methods, or techniques of counterterrorism investigations that were utilized in Operation Flex against particular subjects. This

category includes previously undisclosed information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative sources and methods, were used in a counterterrorism investigation of a particular person, the reasons such methods were used, the status of the use of such sources and methods, and any results derived from such methods

31. The disclosure of the information in this category reasonably could be expected to cause significant harm to the national security. The disclosure of sources and methods used in a particular investigation would reveal not only the identities of particular subjects but the steps taken by the FBI in counterterrorism investigations. FBI sources and methods for investigating potential terrorist threats are of the utmost significance, because the FBI's top priority is to detect and prevent terrorist attacks. The disclosure of sources and methods, such as confidential human sources, the existence of surveillance, and the use of other techniques, would provide a roadmap to adversaries as to how the FBI goes about this vital task. For these reasons, disclosure of the sources and methods used by the FBI in a particular counterterrorism investigation, including in Operation Flex, reasonably could be expected to cause significant harm to national security.

CONCLUSION

32. For the reasons set forth above, based on my personal consideration of the matter, I have determined that disclosure of the information in the three categories described above reasonably could be expected to cause significant harm to national security. I refer the Court to my classified declaration, submitted solely for *in*

camera, ex parte review, for further details concerning the information subject to the Attorney General's privilege assertion.

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

DATE: [7/25/11]

/s/ MARK F. GIULIANO
MARK F. GIULIANO
Assistant Director
Counterterrorism Division
Federal Bureau of Investigation
Unites States Department of Justice

APPENDIX G

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

Case No.: SA CV 11-00301 CJC (VBKx)

YASSIR FAZAGA, ALI UDDIN MALIK, YASSER ABDELRAHIM, PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION; UNITED STATES OF AMERICA; ROBERT MUELLER, DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION, IN HIS OFFICIAL CAPACITY; STEVEN M. MARTINEZ, ASSISTANT DIRECTOR IN CHARGE, FEDERAL BUREAU OF INVESTIGATION'S LOS ANGELES DIVISION, IN HIS OFFICIAL CAPACITY; J. STEPHEN TIDWELL; BARBARA WALLS; PAT ROSE; KEVIN ARMSTRONG; PAUL ALLEN; DOES 1-20, DEFENDANTS

Filed: Sept. 13, 2011

FIRST AMENDED COMPLAINT
CLASS ACTION

Before: HONORABLE CORMAC J. CARNEY.

PRELIMINARY STATEMENT

1. This case concerns an FBI-paid agent provocateur who, by misrepresenting his identity, infiltrated several mainstream mosques in Southern California, based on the FBI's instructions that he gather information on Muslims.

2. The FBI then used him to indiscriminately collect personal information on hundreds and perhaps thousands of innocent Muslim Americans in Southern California. Over the course of fourteen months, the agents supervising this informant sent him into various Southern California mosques, and through his surveillance gathered hundreds of phone numbers, thousands of email addresses, hundreds of hours of video recordings that captured the interiors of mosques, homes, businesses, and the associations of hundreds of Muslims, thousands of hours of audio recording of conversations —both where he was and was not present—as well as recordings of religious lectures, discussion groups, classes, and other Muslim religious and cultural events occurring in mosques.

3. This dragnet investigation did not result in even a single conviction related to counterterrorism. This is unsurprising, because the FBI did not gather the information based on suspicion of criminal activity, but instead gathered the information simply because the targets were Muslim.

4. Ironically, the operation ended when members of the Muslim communities of Southern California reported the informant to the police because of his violent rhetoric, and ultimately obtained a restraining order against him.

5. After this, the informant's identity was revealed, first in court documents where the FBI and local law enforcement revealed his role, and then through his own statements which were reported widely in the press.[1]

---

[1] *See, e.g.*, Jerry Markon, *Tension grows between Calif. Muslims, FBI after informant infiltrates mosque*, WASH. POST (Dec. 5, 2010); Gillian Flaccus, *Calif. case highlights use of mosque informants*,

6. By targeting Muslims in the Orange County and Los Angeles areas for surveillance because of their religion and religious practice, the FBI's operation not only undermined the trust between law enforcement and the Southern California Muslim communities, it also violated the Constitution's fundamental guarantee of government neutrality toward all religions.

7. The First Amendment guarantees that no person should be singled out for different treatment by government because of his or her religion. "The First Amendment mandates governmental neutrality between religion and religion. The State may not adopt programs or practices which aid or oppose any religion. This prohibition is absolute." *Larson v. Valente*, 456 U.S. 228, 246 (1982) (quotations and citations omitted).

8. By this class action, Plaintiffs seek injunctive relief for themselves and the class of individuals whom Defendants subjected to surveillance and gathered identifiable information about because they are Muslim. Specifically, they seek an order requiring the federal government to destroy the information about them which it collected through this unlawful operation. The named Plaintiffs also seek damages for themselves as individuals based on the claims set forth below.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Because this lawsuit alleges violation of the United States Constitution and federal

---

ASSOC. PRESS (Mar. 1, 2009); Matt Coker, *A look at Craig Monteilh*, OC WEEKLY (Mar. 4, 2009); Teresa Watanabe and Paloma Esquivel, *L.A. area Muslims say FBI Surveillance has a chilling effect* L.A. TIMES (Mar. 1, 2009).

statutes, it raises questions of federal law. Because those violations include violations of 42 U.S.C. § 1985 and laws to protect civil rights, this Court also has jurisdiction under 28 U.S.C. § 1343. Because those violations include violations of the Privacy Act, *see* 5 U.S.C. 552a(e)(7), this Court also has jurisdiction under 5 U.S.C. 552a(g)(l)(D).

10. This Court has the authority to grant damages, declaratory and injunctive relief, and any other appropriate relief pursuant to *Bivens v. Six Unknown Agents*, 403 U.S. 388 (1971); 28 U.S.C. 1331; 28 U.S.C. § 1343; 42 U.S.C. § 1985; 42 U.S.C. § 2000bb; 5 U.S.C. 552a; and the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202. A substantial, actual, and continuing controversy exists between the parties, with respect to both the class's claim for injunctive relief in the form of file destruction and the individual claims for damages.

11. Venue is proper in the Central District of California under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims herein occurred in this District.

PARTIES

12. Plaintiff Sheikh Yassir Fazaga is a thirty-eight year-old U.S. citizen born in Eritrea, who moved to the United States at age fifteen and attended high school in Orange County. From about 1998 to the present, Plaintiff Fazaga served as an imam, or religious leader, of the Orange County Islamic Foundation, a mosque in Mission Viejo, California. His duties there have included directing the religious affairs of the mosque, leading prayer, and conducting educational, spiritual, and recre-

ational activities for the entire mosque community and its youth.[2]

13. Plaintiff Ali Malik is a twenty-six year-old U.S. citizen born in Southern California. Malik's parents came to the United States from Pakistan before he was born. From the time of his birth through the events alleged herein, Plaintiff Malik resided in and around Orange County, California. Plaintiff Malik is a practicing Muslim who, from about 2004 through the events alleged herein, regularly attended religious services at the Islamic Center of Irvine ("ICOI"), a mosque in Irvine, California. ICOI is a mainstream mosque and one of the largest mosques in Southern California, with a congregants at times numbering in the thousands, including Muslims from a wide variety of national and ethnic backgrounds.

14. Plaintiff Yasser AbdelRahim, is a thirty-four year-old lawful permanent resident of the United States, who emigrated from Egypt when he was twenty-one years old. Plaintiff AbdelRahim first attended business school in Arizona, then moved to Southern California after he obtained his degree in 1999 to work in business consulting. AbdelRahim is a practicing Muslim and has attended religious services regularly at ICOI since about 2005.

15. Defendant the Federal Bureau of Investigations (FBI) is an agency of the United States government within the meaning of the Privacy Act and the Federal Tort Claims Act. It maintains records on individual whom its agents have investigated, including Plaintiffs

---

[2] Plaintiff Fazaga's legal name is Yassir Mohammed; but he uses the name "Fazaga" in all his personal and professional dealings.

and the putative class they seek to represent. The FBI is sued for injunctive relief only.

16. Defendant Robert Mueller is the Director of the FBI. In that capacity he is responsible for the direction and oversight of all operations of the FBI, including the retention of records arising out of the investigations of FBI agents. He is sued in his official capacity for injunctive relief only.

17. Defendant Steven M. Martinez is the Assistant Director In Charge of the FBI's Los Angeles Field office.[3] In that capacity, he is responsible for the direction and oversight of all operations of the FBI in Los Angeles and Orange Counties, including the retention of records arising out of the investigations of FBI agents in his jurisdiction. He is sued in his official capacity for injunctive relief only.

18. Upon information and belief, Defendant Kevin Armstrong was, at all times relevant to this action, employed by the FBI, and acting within the scope of his employment, as a Special Agent assigned to the Orange County area, and a handler for Craig Monteilh. Agent Armstrong met with Monteilh repeatedly and on a regular basis during the time period at issue in this lawsuit. He directed Craig Monteilh to indiscriminately gather information on the Muslim community in Orange County, and personally supervised and directed Monteilh's surveillance activities as described herein.

---

[3] In addition to its national headquarters and various specialized facilities operations, the FBI maintains 56 field offices in major cities, nearly 400 smaller offices called resident agencies in cities and towns across the nation, and more than 60 international offices in U.S. embassies worldwide.

19. Upon information and belief, Defendant Paul Allen was, at all times relevant to this action, employed by the FBI, and acting within the scope of his employment, as a Special Agent assigned to the Orange County area, and a handler for Craig Monteilh. Agent Allen met with Monteilh repeatedly and on a regular basis during the time period at issue in this lawsuit. He directed Craig Monteilh to indiscriminately gather information on the Muslim community in Orange County, and personally supervised and directed Monteilh's surveillance activities as described herein.

20. Defendant J. Stephen Tidwell, at all times relevant to this action, was an employee of the FBI and acting within the scope of his employment. Defendant Tidwell served as the Assistant Director in Charge of the FBI's Los Angeles Field Office from August 2005 to December 2007, in which capacity he supervised operations in the Central District of California. Upon information and belief, Defendant Tidwell authorized the search for an informant to go into mosques in Orange County to collect information on Muslims, authorized the selection of Craig Monteilh as that informant, authorized the nature and scope of the operation and its targeting of Muslims, read Monteilh's notes of his activities, and authorized and actively directed the actions of Agents Armstrong, Allen, Rose, Walls and other agents in the handling of Monteilh at all times relevant in this action, for the purpose of surveilling Plaintiffs and other putative class members because they were Muslim.

21. Upon information and belief, Defendant Barbara Walls was, at all times relevant to this action, employed by the FBI, and acting within the scope of her employment as Special Agent in Charge of the Santa Ana

branch office, one of ten satellite offices of the FBI's Los Angeles field office, where she was one of the direct supervisors of Agents Allen, Armstrong, and Rose. Upon information and belief, Defendant Walls was regularly apprised of the information Agents Armstrong and Allen collected through Monteilh; directed the action of FBI agents on various instances based on that information; and actively monitored, directed, and authorized the actions of Agents Armstrong and Allen and other agents at all times relevant in this action, for the purpose of surveilling Plaintiffs and other putative class members because they were Muslim. Eventually, she ordered that Agents Armstrong and Allen cease using Monteilh as an informant because she no longer trusted him.

22. Upon information and belief, Defendant Pat Rose was, at all times relevant to this action, employed by the FBI and acting in the scope of her employment as a Special Agent. Upon information and belief, Agent Rose was assigned to the FBI's Santa Ana branch office, where she supervised the FBI's Orange County national security investigations and was one of the direct supervisors of Agents Allen and Armstrong. Upon information and belief, Defendant Rose was regularly apprised of the information Agents Armstrong and Allen collected through Monteilh; directed the action of FBI agents on various occasions based on that information; and actively monitored, directed, and authorized the actions of Agents Armstrong and Allen and other agents at all times relevant in this action, for the purpose of surveilling Plaintiffs and other putative class members because they were Muslim. Agent Rose also sought additional authorization to expand the scope of the surveillance program described herein, in an effort to create a

Muslim gym that the FBI would use to gather yet more information about the class.

23. Defendant Does 1-20 are agents of the Federal Bureau of Investigation and United States Department of Justice, whose identities are not yet known to Plaintiffs, who authorized, directed, and actively monitored the actions alleged herein in order to engage in surveillance of the Plaintiffs and putative class members because they were Muslim.

FACTUAL ALLEGATIONS

FBI Focus On Islam Since 2001

24. Since September 11, 2001, the FBI has focused much of its counterterrorism efforts on broad investigations in the Muslim communities of the United States. In the weeks and months following 9/11, the United States detained hundreds of "suspects" across the country, the vast majority of whom were Muslim. Over the next few years, the FBI engaged in a program to conduct interviews of thousands of individuals who had immigrated to the U.S. from countries in which intelligence allegedly indicated al-Qaeda operated, a burden that fell overwhelmingly on Muslims.[4]

25. In January 2003, the FBI ordered its field supervisors to count the number of mosques and Muslims in their jurisdictions to aid in counterterrorism investigations.[5]

---

[4] *Homeland Security: Justice Department's Project to Interview Aliens after September 11, 2001*, U.S. Gen. Accounting Office, G.A.O. No. GAO-03-459 (April 2003) *available at* http://www.gao.gov/new.items/d03459.pdf.

[5] Eric Lichtblau, *F.B.I. Tells Offices to Count Local Muslims and Mosques*, N.Y. TIMES (Jan. 28, 2003), *available at* http://www.nytimes.com/2003/01/28/politics/28MOSO.html.

26. Starting in 2002 and continuing through 2005, the FBI engaged in a program of monitoring radiation levels across the country, including at more than one hundred "Muslim sites," though officials indicated that religion was not the "only criterion." According to one official, Muslim sites were picked because, in the past, terrorists or people close to them had tended to live in Muslim areas or attend local mosques.[6]

27. In a 2006 briefing to reporters, the FBI official second-in-command over the National Security Branch displayed a map of the San Francisco area showing where Iranian immigrants were clustered—and where, he said, an F.B.I. squad was "hunting."[7]

Evolution of FBI Policies on Use of Religion in Investigation

28. The FBI has been accused of targeting people based on their First Amendment activity before. During the 1960s and 1970s, domestic intelligence-gathering activities by the FBI came under increasing scrutiny, culminating in the "Church Committee," a Senate Select Committee that investigated the FBI's COINTELPRO operation.

---

[6] Kevin Bohn and Jeanne Meserve, *Officials: Muslim sites subject to secret monitoring for radiation*, C.N.N. (Dec. 24, 2005), *available at* http://articles.cnn.com/2005-12-23/us/nuke.monitoring_1_radiation-levels-_radioactive-material-fbi-program; Mary Beth Sheridan, *Mosques Among Sites Monitored for Radiation*, WASH. POST (Dec. 29, 2005).

[7] Scott Shane and Lowell Bergman, *F.B.I Struggling to Reinvent Itself to Fight Terror*, N.Y. TIMES (Oct. 9, 2006), *available at* http://www.nytimes.com/2006/10/10/us/10fbi.html.

29. In 1976, the Church Committee wrote that "The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret Informants . . . has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity. Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable."[8]

30. After uncovering rampant abuses in the FBI's domestic intelligence programs, the Church Committee recommended a series of reforms that were ultimately adopted, including new laws to restrict domestic surveillance for national security purposes under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, and guidelines issued by Attorney General Edward Levi (known as "Attorney General's Guidelines") to regulate domestic intelligence-gathering by the FBI.

31. The Levi Guidelines restricted the FBI's domestic intelligence collection authorities to investigations of

---

[8] *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, "Book II: Intelligence Activities and the Rights of Americans," at 5, U.S. Senate, 94th Cong., 2nd Sess. (Apr. 26, 1976), *available at* http://www.aarclibrary.org/publib/church/reports/book2/html/ChurchB2_0009a.htm.

potential violations of federal law, and limited the use of specific investigative techniques, including informants. The Guidelines allowed the FBI to conduct full domestic security investigations only on the basis of "specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law . . . "[9] More limited Preliminary Investigations could be authorized for 90 days based on receipt of "allegations or other information that an individual or group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law," but only to determine whether there is a sufficient factual basis for opening a full investigation.[10]

32. In 2002, Attorney General John Ashcroft revised the Guidelines for General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, respectively, significantly reducing or eliminating the requirement of a factual basis to believe federal crimes would be committed before the FBI could initiate investigations.[11] Significant changes to the General Crimes guidelines included expanding the duration and type of investigative techniques that could be utilized in preliminary investigations and creating new authorities for the FBI

---

[9] FBI Statutory Charter: Hearings Before the Senate Committee on the Judiciary, 95th Cong. pt. 1, p. 22 (1978).

[10] *Id.*, at 21.

[11] Attorney General's Guidelines for General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, (May 2002), available at: http://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf and, Attorney General's Guidelines for National Security Investigations and Foreign Intelligence Collection, (Oct. 2003), available at: http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf

to proactively conduct internet and commercial database searches and attend public places and events for the purpose of detecting or preventing terrorist activities, all without any factual basis or allegation indicating a possible violation of federal law. Attorney General Ashcroft said terrorism prevention was the key objective of these new Guidelines, arguing that "Our philosophy today is not to wait and sift through the rubble following a terrorist attack. Rather, the FBI must intervene early and investigate aggressively where information exists suggesting the possibility of terrorism, so as to prevent acts of terrorism. The new guidelines advance this strategy of prevention by strengthening investigative authority at the early stage of preliminary inquiries. Also, even absent specific investigative predicates, FBI agents under the new guidelines are empowered to scour public sources for information on future terrorist threats."[12]

33. In June 2003 the Department of Justice issued "Guidance on the Use of Race by Federal Law Enforcement Agencies," purporting to ban the use of racial or ethnic profiling.[13] This Guidance explicitly failed to include religion as an attribute that could not be used by federal law enforcement officials in making law enforcement decisions. In addition, the Guidance contained

---

[12] Remarks of Attorney General John Ashcroft, Attorney General Guidelines May 30, 2002, at: http://www.justice.gov/archive/ag/speeches/2002/53002agpreparedremarks.htm

[13] Department of Justice Civil Rights Division, "Guidance Regarding the Use of Race by Federal Law Enforcement Authorities, (June 2003), available at: http://www.scribd.com/doc/22092319/DOJ-Guidance-Regarding-the-Use-of-Race-by-Federal-Law-Enforcement-Agencies-June-2003.

broad exemptions for the use of racial profiling in national security and border integrity investigations.[14]

34. In October 2003 Attorney General Ashcroft revised the Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, to authorize the "proactive collection of information concerning threats to the national security, including information on individuals, groups and organizations of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats."[15] These Guidelines authorized the FBI to conduct "threat assessments" without opening preliminary or full investigations—in other words without the required factual basis to justify such investigations.[16]

35. The combined effect of these Guidelines and Guidance was to authorize the FBI to engage in intrusive investigations of First Amendment protected activity, and specifically religious practices, without any factual basis to believe any criminal violations or threat to the national security existed.

36. In 2008, Attorney General Mukasey revised the guidelines further, explicitly eliminating the need for any factual predicate before FBI agents are allowed to conduct a new category of investigation called "assessments." The 2008 revisions allow FBI agents to use an array of intrusive investigative techniques during assessments, including physical surveillance, recruiting

---

[14] *Id.*

[15] Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 2003), available at: http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf

[16] *Id.*, at 3.

and tasking informants, and pre-textual interviews by FBI agents acting in ruse. In response, the FBI revised its internal policy, publishing the FBI's *Domestic Intelligence and Operations Guides* ("DIOG") in December 2008.[17] The DIOG only requires an "authorized purpose" to conduct an assessment, which is defined broadly as "a national security, criminal or foreign intelligence collection purpose."[18] Requiring only an authorized purpose rather than a factual predicate means that the authority to conduct investigations in this category is based on the subjective intent of the agent, rather than any factual information regarding the potential subjects of the assessment establishing suspicion of wrongdoing. Moreover, the DIOG authorizes FBI headquarters and field offices to conduct "Domain Management" assessments to "identify locations of concentrated ethnic communities in the Field Office's domain" and to collect, analyze and map racial and ethnic "behaviors," "cultural traditions," and "life style characteristics" in local communities. FBI Director Robert Mueller issued a broad mandate for FBI offices to "know your domain," which meant "understanding every inch of a given community—its geography, its populations, its economy, and its vulnerabilities."[19] Domain Management assessments appear to be mandated as a matter of course, and require no specific threat or criminal predi-

---

[17] Federal Bureau of Investigation Domestic Investigations and Operations Guide, (Dec. 2008), available at: http://www.muslimadvocates.org/DIOGs_ptl.pdf

[18] DIOG p. 21.

[19] Robert Mueller, Speech to the International Association of Chiefs of Police, San Diego, CA California, Nov. 10, 2008, at: http://www.fbi.gov/news/speeches/using-intelligence-to-protect-our-communities (last visited Sept. 13, 2011).

cate to justify the collection of information regarding the makeup of American communities.

37. Upon information and belief, Defendants operated under the principles set forth in the revised Mukasey Guidelines and DIOGs even before the Attorney General formally issued them. For instance, a 2010 report by the Department of Justice Inspector General revealed that from 2002 to 2006 the FBI engaged in a number of investigations of domestic advocacy groups based on "factually weak" or "speculative" predication.[20] The Inspector General (IG) determined many of the investigations were opened based upon the FBI agents' mere speculation that the individuals or groups might commit some federal crime in the future. The IG determined that most of these investigations did not violate the 2002 Attorney General's Guidelines in effect at the time because all that was required to initiate a preliminary inquiry was "information indicating the possibility of a federal crime," which illustrated "the broad scope of the FBI's authority under the Attorney General's Guidelines to open preliminary inquiries based on extremely limited information, including information about the First Amendment expressions of subjects."[21] Moreover, the IG noted that while the FBI's collection and retention of First Amendment material in these cases often violated the 2002 Guidelines, it would not have violated the revised 2008 Guidelines: "Therefore, some of the violations of policy we found in this review would not

---

[20] Department of Justice Inspector General Review of FBI's Investigations of Certain Advocacy Groups (Sept 2010) (hereinafter "IG Report"): http://www.justice.gov/oig/special/s1009r.pdf (last visited Sept. 13, 2011).

[21] IG Report at 87.

be violations if they occurred today."[22] Additionally, a 2006 New York Times report indicated that FBI Associate Executive Assistant Director Phil Mudd was "pitching" a vague domestic intelligence program called "Domain Management," which vaguely implied "ethnic targeting."[23]

38. Upon information and belief, trainings offered by the FBI have also reflected broad generalizations about Muslims supporting the view that Islam and those who practice it inherently condone violence and should be regarded with suspicion. As recently as 2009, the FBI training for newly recruited agents included a power-point presentation that makes gross generalizations about Islam and Muslims. The presentation included slide entitled "Islam 101" that stated Islam "transforms country's culture into 7th century Arabians ways" and claimed that "it is characteristic of the Arabic mind to be swayed more by words than ideas and more by ideas than by facts." Of the eight books that the training listed as "recommended reading," at least three of them have been widely criticized as setting forth stereotypes about Muslims and Islam. Two listed were by Robert Spencer, founder of the group "Stop the Islamization of America," including his book, "The Politically Incorrect Guide to Islam," which asserts on its cover (reproduced in the training's slides) that "Islam teaches that Muslims must wage war to impose Islamic law on non-Muslim states" and "American Muslim groups are

---

[22] IG Report at 189.

[23] Scott Shane and Lowell Bergman, "FBI Struggling to Reinvent Itself to Fight Terror," NY Times (Oct. 10, 2006), available at http://www.nytimes.com/2006/l0/10/us/10fbi.html (last visited Sept. 13, 2011).

engaged in a huge cover-up of Islamic doctrine and history," and has chapters titled "The Qur'an: Book of War," "Islam: Religion of War" and "Islamic Law: Lie, Steal and Kill," in which it argues that Islam condones violence, criminality, and terrorism.[24]

39. Upon information and belief, William Gawthrop, an FBI senior intelligence analyst who has presented and continues to present trainings at conferences to local law enforcement, has offered trainings or training materials on the "Sources and Patterns of Terrorism in Islamic Law" in which he takes selected quotes from Quran and other Islamic texts out of context to teach that Islam inherently mandates violent action against non-Muslims.

FBI Investigation of Muslims in Orange County, California

40. Approximately 500,000 Muslims live in Southern California, more than 120,000 of them in Orange County, making the area home to the second-largest population of Muslims in the United States.

41. The FBI has surveilled Muslims in Southern California and Orange County for at least several years.

42. In about late 2001 or 2002, the FBI approached at least one Muslim leader asking who the Muslim leaders in the Southern California area are and for a list of mosques.

---

[24] Spencer Ackerman, *FBI 'Islam 1O1' Guide Depicted Muslims as 7th-Century Simpletons*, WIRED (July 27, 2011), available at http://www.wired.com/dangerroom/2011/07/fbi-islam-101-guide (last visited Sept. 13, 2011).

43. In May 2006, Defendant Rose, a supervisor of the FBI's Orange County counterterrorism operations, spoke to the Pacific Club in Irvine about the FBI's counterterrorism efforts. There, she stated that "[t]here are a lot of individuals of interest right here in Orange County."[25] She described recent efforts the FBI had taken in the region: planting bugs and closed-circuit TV cameras, examining computer use and email, and establishing units on both foreigners and domestic suspects. She indicated that the FBI frequently received calls from people who wanted to tell them about situations like a Muslim neighbor who is changing his license plates or someone who has an apartment with only a mattress and five computers, stating, "I can't tell you how many" tips like that paid off. When asked whether citizens should be worried about activist Muslim students at University of California at Irvine, Rose characterized that as a "tough question," but indicated the FBI was aware of large numbers of Muslim students at UCI and the University of Southern California. "We live in Irvine. I can't tell you how many subjects' names come up, and they live right down the street from me," she stated. "I think we need to be concerned with everybody, including our next-door neighbor."[26]

44. In 2006 and 2007, authorities arrested reserve officers who worked at the Strategic Technical Operations Center, an intelligence unit at Camp Pendleton, for stealing classified intelligence documents and providing

---

[25] Frank Mickadeit, *Feds warn O.C. of terror lurking 'down the street'*, THE ORANGE COUNTY REGISTER (May 25, 2005), available at http://www.ocregister.com/news/fbi-194882-county-orange.html (last visited Sept. 13, 2011).

[26] *Id.*

them to local law enforcement. According to reports, the theft ring had operated since 2001, and the documents seized from the participants included more than 100 FBI and Defense Department files, including documents establishing the existence of programs to surveil Muslim communities and mosques in Southern California.[27]

45. Documents obtained by the ACLU of Southern California via the Freedom of Information Act show that the FBI has collected information about the membership of the Shura Council (an association of mosques in the Southern California area), as well as information about activities or events organized at or by mosques or Muslim organizations—including individuals handing out flyers for fundraising, events on political issues such as the war in Iraq or immigration reform, and a wide variety of fundraising efforts.

46. The FBI has sought and continues to seek interviews of hundreds of people in the Southern California Muslim community, often by sending FBI agents to appear unannounced at the homes or workplaces of people to request an interview. During these interviews, FBI agents have often questioned interviewees about religious practices that have no discernible relationship to criminal activity, such as what mosque interviewees attend, how many times a day they pray, who the imam of their mosque is, or what they think of particular religious scholars.

---

[27] Rick Rogers, *Records detail security failure in base file theft*, SAN DIEGO UNION-TRIBUNE (May 22, 2008), available at http://www.signonsandiego.com/uniontrib/20080522/news_1n22theft.html (last visited Sept 13, 2011).

Monteilh's Role in the FBI's Investigation of Muslims

47. In the face of substantial evidence of the FBI's particular focus on investigating Muslims, in June 2006, Los Angeles FBI Assistant Director Stephen Tidwell attended a forum for the Muslim community at the Islamic Center of Irvine ("ICOI"), where he assured an audience of about two hundred people that the FBI would enter mosques only openly to outreach to the community and would not send covert informants into mosques for the purpose of monitoring the Muslim community.[28]

48. At some time prior to July 2006, the FBI hired Craig Monteilh to become a paid informant for them to covertly gather information about Muslims in the Irvine area.

49. In about July 2006, Monteilh requested a meeting with the imam of the Islamic Center of Irvine ("ICOI"). Monteilh told the imam that he was of French and Syrian descent, and that he wanted to embrace his roots by formally converting to Islam. The following Friday, Monteilh attended the *jummah* prayer (the Friday afternoon prayer that is the most important service of the week), where he went before the congregation of hundreds and made a public declaration of his Muslim faith. This declaration, known as *shahadah*, is one of the

---

[28] At some point during the spring of 2007, Agents Armstrong and Allen told Monteilh that the Assistant Director in Charge of the FBI's Los Angeles Field Office had told the Muslim community that there would be no undercover informants placed in mosques at a meeting held only about a month or so before Monteilh had publicly "converted," on their instructions, at the ICOI mosque. They told him that at the time Tidwell made this statement, they had already been looking for someone to send into the mosques, and that Tidwell had approved recruitment of an informant.

five pillars of Islam. After this, Monteilh began going to ICOI on a daily basis, often attending multiple prayers a day. About a week later, he began using the Muslim name Farouk al-Aziz.

50. After taking *shahadah*, Monteilh attended prayers at ICOI on a daily basis. He attended prayers at mosque multiple times per day, and was often waiting for the mosque to open before dawn prayers at about 5 a.m. He also attended classes and special events. He primarily attended ICOI, but also went with some regularity to about five of the other largest mosques in Orange County.

51. Congregants at ICOI generally welcomed Monteilh. People introduced themselves, spoke with him about his conversion and their faith, and offered to help him learn about Islam and Muslims in America. Various congregants offered help by buying him books on Islam, talked with him about the tenets of the religion, and showed him the movements of prayers. Congregants invited him to have meals or tea outside of the mosque to help welcome him to the mosque's community and discuss questions he might have.

52. After several months, Monteilh began wearing traditional Muslim robes and skull caps both at mosque and in public, in place of his "western" clothes.

53. After Monteilh had attended ICOI for some time, Muslim community leaders began to hear concerns voiced by the congregants about Monteilh's behavior. Monteilh engaged people in conversations in which he aggressively probed their views on religion and American foreign policy. Soon leaders began hearing that he was asking people's opinions on *jihad* and its meaning in

Islam, and that he was resisting their claims that Islam did not condone terrorism.

54. Among the many people Monteilh met during his time as an FBI informant were Plaintiffs Fazaga, Malik, and AbdelRahim.

Plaintiff Sheikh Yassir Fazaga

55. Plaintiff Sheikh Yassir Fazaga is a thirty-eight year-old U.S. citizen born in Eritrea, who has lived here since he was a teenager. He attended high school in Orange County. Sheikh Fazaga has an undergraduate degree in Islamic Studies from the Institute of Islamic and Arabic Sciences in Virginia and a masters degree in marriage and family counseling from the California State University of Long Beach, and has taken coursework toward a masters degree in Christian Theology at Loyola Marymount University. From about 1998 to the present, Sheikh Fazaga has served as an imam of the Orange County Islamic Foundation (OCIF), a mosque in Mission Viejo, California. His duties there have included directing the religious affairs of the mosque, leading prayer, and conducting educational, spiritual, and recreational activities for the entire mosque community and its youth.

56. Sheikh Fazaga earned a national reputation for his contemporary American teaching of Islam. He has spoken at numerous conferences, colleges, and other fora both in the United States and abroad on the topics of Islam and the American Muslim. In 2007, he traveled to Romania at the invitation and expense of the U.S. State Department to speak on terrorism, radicalism and extremism. He has also been interviewed for print, television and radio media, including for NBC's Today show on spirituality in America and for a New York

Times article on American imams in which he was featured.[29]

57. Over the years, Sheikh Fazaga's mosque conducted a number of events in conjunction with various other mosques in the area, including ICOI. Sheikh Fazaga was, and still is, concerned about the erosion of civil rights for people in the Muslim community, and he often took actions to advocate on behalf of that issue.

58. On one occasion in early 2006 he attended one such event, which Defendant Stephen Tidwell, Assistant Director in Charge of the Los Angeles FBI Field Office, also attended. At the event, Fazaga asked questions to Tidwell concerning the FBI's use of informants in mosques.

59. Shortly afterward, Sheikh Fazaga came into contact with Craig Monteilh, because Monteilh came to attend prayers and other events at his mosque, OCIF, starting in approximately 2006.

60. Some time after Monteilh began attending his mosque, Sheikh Fazaga hosted a famous Islamic speaker named Yusuf Estes at his mosque. Estes is a former National Muslim Chaplain for the United States Bureau of Prisons, and was a Delegate to the United Nations World Peace Conference for Religious Leaders several years before being invited to speak at the OCIF.

61. A number of Sheikh Fazaga's congregants, including Monteilh, attended the lecture.

---

[29] *See* Neil MacFarquhar, *A Growing Demand for the Rare American Imam*, N.Y. Times (June 1, 2007), available at http://www.nytimes.com/2007/06/01/us/01imam.html (last visited Sept. 13, 2011).

62. Several months after Monteilh first began attending events at OCIF, another member of the OCIF community formally introduced Fazaga to Monteilh.

63. After Monteilh's role as an FBI informant became publicly known in February 2009, a number of Sheikh Fazaga's congregants expressed their dismay to him, because Monteilh had spent a considerable amount of time at the OCIF.

64. Sheikh Fazaga had to spend considerable time counseling his congregants who were afraid that they were being targeted for FBI surveillance because of their faith. He often conducted this counseling away from the mosque and in person, rather than over the telephone, because of his congregants' fear of surveillance.

65. Sheikh Fazaga also observed the trust within and cohesion of his congregation, and of other Muslim communities in Southern California, to be significantly damaged, and that this damage directly undermined the Islamic practice of *jama'ah*, or worship in a congregation. In part because of this, he devoted two whole sermons to addressing the fears of the congregation about surveillance, rather than addressing religious subjects.

Plaintiff Ali Uddin Malik

66. Plaintiff Malik grew up in Orange County, California. When Malik was growing up, his family were strong supporters of the Republican Party. Malik started a young Republicans club at his high school. During high school, Malik aspired to work for the U.S. State Department or elsewhere in government.

67. Plaintiff Malik attended the University of California, Irvine ("UCI") from about 2007 to 2009. While at Irvine, Malik co-founded the Olive Tree Initiative, a

peace-building program through which a culturally and religiously diverse group of UCI students take joint factfinding trips to Israel and Palestine to better understand the Israel-Palestine conflict and report on their findings to the UCI community. Malik and the other founders were recognized for their work with the University of California President's Award for Outstanding Student Leadership, UCI Chancellor's Living Our Values Award, and recognition by the Orange County Human Relations Commission and the U.S. State Department.

68. When Malik was about twenty years old, he developed an interest in religion. His family had always attended the mosque, but he started attending more regularly and trying to study Islam with more seriousness. Malik began wearing traditional robes and head covering when he went to the mosque to pray. He also grew a full, long beard in a traditional fashion. Because Islam encourages Muslims to follow the "Sunnah" or practices of the Prophet Muhammad, who had a beard and required his followers to grow beards, observant Muslim men commonly grow their beards as a part of their religious practice and as a form of modesty, Most observant Muslim men in Orange County wear beards of some sort, and many or most try to grow long beards at some point in their lives. Similarly, many Muslim men wear traditional clothes to pray as part of their religious practice, as a form of modesty. As such, an emulation of the practices of Muhammad is also "sunnah." Malik also found that wearing his clothes and beard in this way helped serve as a reminder of his faith.

69. In about summer 2006, as part of his efforts to study Islam more seriously, Malik attended a six-week

summer course on Islam at Dar al-Mustafa, a seminary in Yemen. Islam emphasizes the importance of gaining religious knowledge, and encourages its adherents to seek knowledge, so much so that for Muslims gaining religious knowledge is a faith practice in and of itself. Dar al-Mustafa is a mainstream religious school whose leaders are internationally known in the Muslim community for advocating justice, equality, and peaceful co-existence between religious groups, and have been active in interfaith efforts in these areas with religious leaders of other faiths. Upon information and belief, the school and its leaders enjoyed a similar reputation with the United States government and the FBI. At the time Malik attended the summer course, both Yemen and Dar al-Mustafa were popular places for American Muslims who wanted to pursue Arabic language or religious studies abroad for a variety of reasons: Southern Yemen, where Dar al-Mustafa is located, was known for its spiritual Sufi religious scholarship, for having a clear and eloquent form of the Arabic language, and for being scenic and affordable, if slightly rustic. Plaintiff Malik attended ICOI and was present when Monteilh took *shahadah* in about July 2006. Plaintiff Malik, along with many other congregants, approached Monteilh after he took *shahadah*, offering his well-wishes and assistance.

70. In about August 2006, the imam at ICOI asked Plaintiff Malik to teach Monteilh how to pray and to guide him through the basics of Islam.

71. At the imam's request, Plaintiff Malik approached Monteilh. Malik talked with Monteilh about the basics of Islam, including the basic tenets, how to pray, and the development of faith. Monteilh asked for Malik's cell phone number and email address, which Ma-

lik provided. He tried to offer Monteilh support and welcome him in the community, and talked about inviting him over to his family's house for dinner.

72. To help Monteilh learn about Islam, Plaintiff Malik gave him a very basic book on the religion. The book is commonly used to teach Sunday school classes to children, and Malik knew that his father had taught Sunday school and had used the same book.

73. Monteilh talked frequently with Malik at the mosque. He also suggested that they talk at a nearby gym, which they did in part because Monteilh worked out there. Shortly after their meeting, Monteilh began asking Malik things that made Malik uncomfortable. At one point Monteilh asked Plaintiff Malik what would happen if someone went up to the imam at ICOI and told him they wanted to blow themselves up. Plaintiff Malik replied that the imam would think this person was crazy. Monteilh persisted, and asked Plaintiff Malik if there were other imams in the area that would respond to someone who wanted to blow themselves up. Plaintiff Malik told Monteilh that there are no such imams or mosques in Southern California as far as he knew.

74. On another occasion, Monteilh asked Malik about *jihad*, citing specific pages in the children's book Malik had given him that mentioned jihad. When Malik answered that *jihad* meant a "struggle," and that the concept referred to the spiritual struggle to purify oneself, Monteilh pressed him about whether it meant physical violence, and resisted Malik's answer that it did not.

75. These conversations deeply concerned Malik and made him very uncomfortable around Monteilh. Malik thought that Monteilh had strange ideas about Is-

lam from movies or media, and urged him to go talk to the imam so that the imam could guide him.

76. When Monteilh persisted in talking with Malik about his violent ideas, Malik began trying to avoid Monteilh. He would avoid answering or returning Monteilh's calls, although Monteilh called repeatedly. Malik also began trying to go to the gym at times Monteilh did not attend.

77. Malik also noticed that Monteilh spoke with many others at the mosque. For example, Malik occasionally saw Monteilh praying near meetings of a youth group Malik attended in the mosque's prayer hall. Malik noticed on several occasions that when Monteilh would pray near the group, he would leave his belongings in the prayer hall while he went elsewhere.

78. Finally, Malik stopped attending the mosque altogether because Monteilh was there so often. Malik also stopped attending the mosque in Tustin because he heard that Monteilh had also been seen at that mosque. Malik resumed attending ICOI only after Monteilh began approaching other people and speaking to him less often. Even since returning to the mosque, Malik attends less often than he had before he had contact with Monteilh.

79. In about spring 2007, Monteilh asked Malik about studying Islam abroad. Malik suggested that Monteilh look into the seminary where Malik had studied, Dar al-Mustafa, which Malik had enjoyed very much.

Plaintiff Vasser AbdelRahim

80. Plaintiff AbdelRahim was another victim of Monteilh's dragnet surveillance of Muslims in Irvine. AbdelRahim started attending ICOI in about 2005. Shortly afterwards, he rented a room in a large house

where a friend he met through the mosque lived. Over the next few months, two other mutual friends from ICOI, and AbdelRahim's brother, moved into the house as other roommates left. All five of the housemates were, like AbdelRahim, of Egyptian origin.

81. In about July 2006, one of AbdelRahim's roommates told him about a guy who had taken *shahadah* at the mosque. The following Saturday, they saw Monteilh and introduced themselves, offering to help him learn about Islam if he had any questions. Monteilh said that he appreciated it and took their phone numbers.

82. Shortly afterward, Monteilh called AbdelRahim and began socializing with AbdelRahim and his roommates. They talked, went out to get coffee, and soon AbdelRahim invited Monteilh to their house for *iftar* (a meal eaten during Ramadan). Monteilh began to spend time with them at their house watching TV or playing X-box. AbdelRahim and his roommates also tried to help Monteilh feel welcome by introducing him to other people in the Muslim community.

83. Initially, Monteilh talked with AbdelRahim and his roommates about a variety of innocuous topics—not only about Islam, but about politics, world affairs, movies, and sports. At some point, however, Monteilh began asking questions about *jihad,* again with a focus on violence. AbdelRahim found this odd, and responded that Monteilh should not concern himself with that, but instead should concentrate on developing his faith, and should talk to the imam at ICOI if he had questions about the meaning of *jihad.* However, Monteilh persisted in raising the subject. AbdelRahim eventually became worried that Monteilh had asked him several times about *jihad,* particularly when he heard from several of

his friends at the mosque that Monteilh had made similar inquiries with them. AbdelRahim also noticed that Monteilh guided conversations to political subjects like the wars in Iraq and Afghanistan, and would say inflammatory things that seemed aimed at eliciting agreement or angry responses from others.

84. Shortly afterward, a friend of AbdelRahim reported to him that Monteilh had asked the friend to coffee to discuss a personal issue, but then started asking particularly pointed questions about *jihad*. Upon hearing this, AbdelRahim confronted Monteilh. AbdelRahim told Monteilh that if someone was teaching him this view of *jihad*, then he needed to find another teacher.

85. After this conversation, AbdelRahim stopped speaking with Monteilh or returning his calls. Over the next several months, AbdelRahim noticed that Monteilh was spending time with different people at the mosque, and AbdelRahim warned a few of them about his concerns regarding Monteilh.

The FBI's "Dragnet" Approach

86. The interactions between Monteilh and Plaintiffs Fazaga, Malik, and AbdelRahim were part of a broader pattern of dragnet surveillance that Monteilh engaged in at the behest of his FBI handlers. Two FBI Special Agents instructed Monteilh to gather information on Muslims in general, and instructed him to adopt strategies of information-gathering and surveillance that ensured that he would obtain that information in an indiscriminate manner, such that Plaintiffs and numerous other people were surveilled solely due to their religion. They also provided Monteilh with the tools needed to conduct this indiscriminate surveillance, including sophisticated audio and video recording devices.

Again, their instructions ensured that the surveillance tools would target people solely due to their religion.

87. Monteilh's handlers at the FBI were FBI Special Agent Kevin Armstrong and FBI Special Agent Paul Allen. Agents Armstrong and Allen supervised all of Monteilh's work with the FBI. The FBI paid Monteilh for the duration of his work for Agents Armstrong and Allen, in amounts ranging from about $6,000 to over $11,000 per month.

88. Agents Armstrong and Allen told Monteilh that the FBI used the name "Operation Flex" for the surveillance program that used him, and used that term repeatedly. Agents Armstrong and Allen told Monteilh that the name referenced him, since he operated under the cover of a fitness consultant. But they also told Monteilh that Operation Flex was a broader surveillance program that went beyond just his work.

89. The central feature of the FBI agents' instructions to Monteilh was their directive that he gather information on Muslims, without any further specification. Agents Armstrong and Allen did not limit Monteilh to specific targets on which they wanted information. On the contrary, they repeatedly made clear that they were interested simply in Muslims. To the extent they differentiated within that group, they held a heightened interest in Muslims who were particularly religious.

90. When Agents Armstrong and Allen first sent Monteilh to meet the imam at ICOI and began infiltrating the Muslim community, they gave him no specific targets, but instead told him to gather as much information on as many people in the Muslim community as possible. Agent Allen told Monteilh, "We want to get as many files on this community as possible." Agents Arm-

strong and Allen told Monteilh that the United States was five to ten years behind Europe in the extent of Islamic presence, and that they needed to build files on as many individuals as possible so that when things started to happen, they would know where to go. They said they were building files in areas with the biggest concentrations of Muslim Americans—New York; the Dearborn, Michigan area; and the Orange County/Los Angeles area.

91. In addition to information about the membership of each mosque, Agents Armstrong and Allen instructed Monteilh to get the names of all board members, imams, people who taught classes at the mosques, and other leadership figures within the mosques.

92. Over the course of the investigation, Agents Armstrong and Allen sent Monteilh to about ten mosques to conduct surveillance and audio recording in each one. Monteilh spent the most time at ICOI, which he attended daily, but spent significant time at other mosques, including the Orange County Islamic Foundation mosque in Mission Viejo, Durol Falah in Tustin, Omar al-Farouq mosque in Anaheim, Islamic Society of Orange County in Garden Grove, Al-Fatiha in the West Covina/Azusa area, the mosque in Lomita, and King Fahd mosque in Culver City. For about five or six months Monteilh went at least once a week to each of these mosques, and would go to as many as four different mosques in a day to meet with and talk to people, if not to pray.

93. Agents Armstrong and Allen initially told Monteilh he would make his first contact with the community by attending services at a mosque in Anaheim, but then instructed him to attend ICOI instead because it was closer to where he lived, so he could spend more time there.

94. Agents Armstrong and Allen also informed Monteilh that the surveillance program was itself spread indiscriminately across the area's mosques. Electronic surveillance equipment was installed in at least eight area mosques including ICOI, and mosques in Tustin, Mission Viejo, Culver City, Lomita, West Covina, and Upland. They told him at one point that they could get in a lot of trouble if people found out what surveillance they had in the mosques, which Monteilh understood to mean that they did not have warrants. Nonetheless, Agent Armstrong told Monteilh that the FBI had every mosque in the area under surveillance—including both the ones he went to and the ones he didn't.

95. Upon information and belief, Agents Allen and Armstrong caused such electronic surveillance equipment to be installed at the Mission Viejo mosque and used it to monitor conversations of Plaintiff Yassir Fazaga, including conversations held in parts of the mosque not open to the public, including Sheikh Fazaga's office.

96. Apart from the electronic surveillance program, Agents Armstrong and Allen also directed their surveillance at people on the basis of their religion by instructing Monteilh to look for and identify to them people with certain religious backgrounds or traits, such as anyone who studied *fiqh* (a strand of Islamic law concerning morals and etiquette), who was an imam or sheikh; who went on *Hajj;* who played a leadership role at a mosque or in the Muslim community; who expressed sympathies to *mujahideen;* who was a "white" Muslim; or who went to an Islamic school overseas.

97. Even with respect to these categories of Muslims, Monteilh's handlers did not tell him to limit the information he collected to those people. Agents Arm-

strong and Allen would occasionally instruct Monteilh to spend more time with or find out more about particular people he identified, but these were always people Monteilh had identified to them during the course of the operation, not people who had been targeted from the outset.

98. Agents Armstrong and Allen also instructed Monteilh to focus on Muslim youth by keeping an eye out for people who tended to attract young Muslims. They instructed him to identify and gather information on such people. For example, Monteilh told them about a popular youth group on Tuesdays at ICOI run by the imam. Students from the Muslim Student Union at the University of California, Irvine ("UCI") would attend. On many occasions, Monteilh recorded the youth group meetings at ICOI by leaving his possessions, including the recording key fob, near where the group met in the prayer hall so that all of their discussions could be recorded. Monteilh did this by going into the prayer hall during their meetings to pray, and then leaving behind his possessions as if he had forgotten them or just chosen to leave them there while he did other things. Monteilh would go to another part of the mosque or the courtyard, and return sometime later to collect his things. Monteilh told his handlers he did this in his written reports. His handlers never instructed him to stop this practice, and instead repeatedly discussed with him the contents of the recordings obtained in this manner.

The FBI's Surveillance Strategies

99. The FBI agents instructed Monteilh to engage in a number of surveillance strategies, all of which served to gather information on Muslims in an indiscriminate manner.

100. After Monteilh agreed to work as a confidential informant and underwent some training under the supervision Agents Armstrong and Allen, Agents Armstrong and Allen instructed him to make the appointment to see the imam at the ICOI. Once Monteilh had taken *shahadah* and began attending both ICOI and other mosques, Agents Armstrong and Allen instructed him to gather information on the Muslims at the mosques.

101. Agents Armstrong and Allen instructed Monteilh to obtain information through various methods. They told him to take every opportunity to meet people, get their contact information, meet them privately to get to know them, find out their background, find out their religious and political views, and get any information about them that he could to pass on to the FBI.

102. As a result, over the time he spent at ICOI and other mosques Monteilh did not focus on any particular group of people, such as those who may have engaged in criminal activity or even those from a particular country, but instead socialized widely with different groups and individuals. ICOI is a multi-lingual, multi-ethnic mosque, with separate social groups that form around common language or country of origin. Monteilh surveilled people from every social group regardless of their ethnic origin or dominant language.

103. Pursuant to his handlers' instructions, Monteilh went out of his way to engage all of these different groups, even when he had no natural connection to them. For example, he attended religion classes given in Arabic even when he did not speak Arabic, and questioned 17 and 18 year olds about religious doctrine and politics, when a stranger in his forties might be expected to ask such questions of adults, not youth. Similarly, Monteilh

spent significant time with a group of Egyptians, a group of Pakistanis and Indians, a group from Syria and Lebanon, and with the younger, second-generation social groups (generally identified as "Muslim Students Union," or MSU, in reference to on-campus Muslim organizations). Within each group, he spoke to large numbers of people so as to probe their views on religion, politics and violence, and then report them back to his handlers at the FBI.

104. Within these groups, Monteilh tended to focus more heavily on people who were more religious; people who came to the mosque only to attend Friday prayers were less likely to be recipients of his attention.

105. Agents Armstrong and Allen also gave Monteilh a standing order to gather information on Muslims' charitable giving. They instructed him to collect any pamphlet or brochure at any mosque that concerned charitable donations, to inquire of Muslims about which charities and Islamic schools to give to, and to then pass on the names of the charities and Islamic schools to them.

106. Monteilh's handlers also instructed him to attend Muslim fundraising events, to interact with the community and gather information, to identify people who attended and who they came with, and, if there were any speakers, to record what those speakers said.

107. Agents Armstrong and Allen also asked Monteilh to collect information on the travel plans of Muslims in the community. They told him that they shared this information with the Department of Homeland Security so as to be able to monitor or search people during their travels.

108. Monteilh's handlers also instructed him to attend lectures by Muslim scholars and other guest speakers. Because Monteilh's handlers wanted to know both what the lecturers said and who attended these lectures, they equipped Monteilh with a video surveillance device that had a camera in a shirt button, so that he could both record lectures and film attendees socializing. Monteilh also collected license plate numbers from the parking lots to identify those who attended.

109. In keeping with his handlers' orders, Monteilh also attended classes at the mosque so as to obtain more information on Muslim community members. For example, he attended an Arabic language class at ICOI from about December 2006 to March 2007. On his handlers' instructions, he obtained and provided them with the lists of the individuals who attended the class. Monteilh also attended a course in *fiqh,* and obtained and provided the class list to his handlers, as per their instructions.

110. Agents Armstrong and Allen also instructed Monteilh to attend *fajr* (dawn) prayers, which are held about 4 a.m., or *ishaa* (late) prayers, which are held about 9:30 p.m. Agents Armstrong and Allen told him that people who attended prayers very early in the morning or late at night, and especially both, were very devout and therefore more suspicious. They instructed him to obtain the names and the license plate numbers of individuals who attended these prayers. Agents Armstrong and Allen increased his pay when he agreed to go to *fajr* prayer four days a week.

111. Agents Armstrong and Allen also instructed Monteilh to memorize certain *ayas* and *surahs* (verses and chapters from the Quran) and to ask Muslims about them. They said they had picked these verses because

they believed them to be susceptible to a "jihadist" interpretation, so that people's reactions to them would help discern who was and was not a threat. They told Monteilh that discussions about these verses would elicit responses that could be used to justify additional surveillance measures.

112. Agents Armstrong and Allen also expressed interest in any Muslims who followed websites that the agents believed were "jihadist," including *Mission Islam.com* and *CagePrisoners.com* (a site devoted to raising awareness about the detainees at Guantanamo Bay). Agent Allen told Monteilh to encourage people he spoke with to go to these websites because they could document people's visits to the website and use that either to pressure them to become informants or to justify further surveillance on them.

113. Agents Armstrong and Allen also encouraged Monteilh to bring up in conversation certain Muslim scholars and thinkers whom they believed were extremist, so as to elicit people's views on them. The scholars they instructed him to discuss included a number of Islamic scholars who, at the time, were both widely popular and moderate, such as Sheikh Suhaib Webb and Yusef Estes.

114. Monteilh also used his cover as a fitness consultant to gather information on the Muslims with whom he interacted. During his time working on Operation Flex, Monteilh told people in the Muslim community that he worked as a fitness consultant. In about November 2006, Agent Allen instructed Monteilh to start going to the gym to work out with people he met from the Muslim community, in order to get close to them and obtain information about them. Again, Monteilh's handlers did

not limit the scope of their instructions; the directive included anyone from any mosque without any specific target, for the purpose of collecting as much information as possible about Muslims in the community. Pursuant to these instructions, Monteilh worked out with Muslims in various gyms around the Orange County area and elicited a wide variety of information, including travel plans, political and religious views.

115. The goal of these conversations was to obtain compromising information that his handlers could use to pressure the Muslims with whom Monteilh interacted into providing information or becoming informants. Monteilh recorded these conversations using the equipment on his key fob or cell phone. This surveillance was so fruitful that Monteilh's handlers eventually told him they were seeking approval to have him open a Muslim gym.

116. Agents Armstrong and Allen talked repeatedly with Monteilh about obtaining new informants within the Muslim community, primarily by getting information on potential informants that could be used against them if they refused to inform—such as immigration issues, sexual activity, business problems, or crimes like drug use. Agents Armstrong and Allen instructed Monteilh to pay attention to people's problems, to talk about and record them, including marital problems, business problems, and petty criminal issues. Agents Armstrong and Allen on several occasions talked about different individuals that they believed might be susceptible to rumors about their sexual orientation, so that they could be persuaded to become informants through the threat of such rumors being started.

117. Agents Armstrong and Allen also often spoke with Monteilh about a maxim that "everybody knows

somebody." They explained that if someone is from Afghanistan, that meant that they would likely have some distant member of their family or acquaintance who has some connection with the Taliban. If they are from Lebanon, it might be Hezbollah; if they are from Palestine, it might be Hamas. By finding out what connections they might have to these terrorist groups, no matter how distant, they could threaten the individuals and pressure them to provide information, or could justify additional surveillance.

118. Agents Armstrong and Allen also instructed Monteilh to engage in acts that would build his reputation as a devout Muslim who had access to black market items. On one occasion, Agents Armstrong and Allen instructed Monteilh to provide Vicodin to a person whose father was sick in a foreign country. On another occasion, Agent Allen instructed Monteilh to provide prescription anabolic steroids to another two individuals to similarly further his credibility, which he did.

119. During their regular meetings with Monteilh, Agents Armstrong and Allen also showed him photographs of Muslims from the community, taken from many of the methods identified above (e.g. at the gym, at fajr prayer, etc.), asked him to identify the people in those photographs, and then directed him to provide as much information as possible about each person, including what mosque they attended, their ethnicity or country of origin, the languages they spoke, the people they associated with, what kind of car they drove, their occupation or whether they were a student, as well as any other information Monteilh could obtain.

120. One theme ran throughout all of these different surveillance gathering strategies: Agents Armstrong

and Allen expressed interest in gathering information only on Muslims, and they set aside any non-Muslims who were identified through surveillance Monteilh performed. For example, on several occasions when Agents Armstrong and Allen asked Monteilh to identify individuals from photographs taken by surveillance cameras at the entrances to gyms, they presented him with photographs of individuals who were not Muslim—usually Latino—who Monteilh had spoken to or who had simply helped him lift weights. Each time Monteilh indicated to Armstrong and Allen that the individual identified was not a Muslim, they discarded the picture.

121. Indeed, both Agent Armstrong and Agent Allen, as well as other agents, explicitly told Monteilh that Islam was a threat to America's national security.

The FBI's Surveillance Tools

122. Agents Armstrong and Allen recorded information about virtually all of the people with whom Monteilh interacted in several different ways—through audio recording, video recording, extensive review of Monteilh's handwritten notes about all aspects of his daily interactions, and a dragnet program to obtain cellphone numbers, email addresses, and information about internet usage.

123. Upon information and belief, virtually all of Monteilh's interactions with Muslims in the mosques were recorded by audio, video, or both. The recordings were then transcribed and reviewed by officials within the FBI. Agent Allen told Monteilh that there was a team transcribing all of his recorded conversations.

124. Agents Armstrong and Allen instructed Monteilh that because of his criminal background, all infor-

mation he collected would have to be recorded. After about September 2006, Armstrong and Allen gave Monteilh a cell phone and two key fobs (which resembled the remote controls for car locks) with audio recording devices in them, and which Monteilh used to record all day, every moment he worked undercover, regardless of whom he was meeting or what was discussed.

125. People at ICOI noticed that Monteilh would often forget his keys, so that they would be delivered to the imam's office. People joked about Monteilh frequently forgetting his keys, and for having his keys out during lectures and conversations, even if he had to get them out after he sat down.

126. In fact, Monteilh utilized the trick of leaving his keys around the mosque to allow audio recording of conversations to take place even when he was not present.

127. On several occasions, Monteilh also left the recording devices in locations in mosques in the area. For example, in a large mosque in Culver City, Monteilh several times attended with a friend who changed in the office from business clothes to more traditional dress before they went into the mosque to pray. Monteilh left his keys in the office so that the key fob would record staff and board members who came in and talked, then retrieved his keys from the office when they were finished in the mosque. Monteilh did this several times, and in several different mosques. Agents Armstrong and Allen received the notes where Monteilh said he did this but never instructed him to stop.

128. Monteilh's recording activity was not limited to audio. Beginning in about February 2007, on numerous occasions Agents Armstrong and Allen outfitted Monteilh with video surveillance equipment that recorded

through a camera hidden in a button in the front of his shirt, while recording audio as well. Toward the end of his assignment, Agents Armstrong and Allen had equipped Monteilh to use this video surveillance as often as several days per week.

129. Agents Armstrong and Allen instructed Monteilh to use the video camera for various specific purposes, including to capture the internal layout of mosques, to film basketball or soccer games to see who associated with whom, to film guest lectures at mosques to see what was said and who attended, and to record the interiors of people's houses. Monteilh's handlers at various times instructed him to open particular doors in homes or mosques and film the room behind.

130. Agents Armstrong and Allen also used Monteilh's activities to gather telephone and cell phone numbers, email addresses, and other electronic information for indiscriminate surveillance.

131. Agents Armstrong and Allen told Monteilh they wanted him to collect contact information, particularly email addresses and phone numbers. At times, they even gave Monteilh quotas to collect contact information for ten new Muslims per day. Agents Armstrong and Allen told Monteilh that they monitored his email and cell phones to obtain the telephone numbers and email addresses of people with whom he corresponded. Agent Allen instructed him to give out his cell phone number widely so that people would call him or give their cell numbers in return, so that the FBI could then collect those numbers. Armstrong and Allen also instructed him to email frequently with people, so that the FBI could collect their email addresses. Agents Armstrong and Allen told Monteilh that they used the cell phone

numbers and email addresses of individuals who contacted him to obtain information from those individuals' phone and email accounts, including the list of people they contacted.

132. Agents Armstrong and Allen told Monteilh that they kept the numbers and emails he collected in a database that could be monitored for international calls, or cross-referenced against phone calls or emails to persons of interest who were believed to be linked to terrorism. Monteilh's handlers also told him that the emails could be used to determine if the person was visiting certain websites, and with whom they were emailing. Monteilh joined email distribution lists for many of the mosques he surveilled, and would forward messages from the mosques to the FBI so they would be informed about events and bulletins, and so they would have the email addresses of anybody else who received the message.

133. Agents Armstrong and Allen also instructed Monteilh to gather all available information, including literature, on events occurring at the mosques. Following these instructions, Monteilh would collect brochures on charities that were distributed in the mosques, visit the mosques' libraries or book areas, collect newsletters and bulletins to see what activities were going on in the mosque, and collect the names of individuals who attended, as well as their cell phone numbers and license plates when possible. He would record this information either electronically or through a system of notes.

134. Agents Armstrong and Allen instructed Monteilh to compose daily notes of his activities and the surveillance he had undertaken. These notes were extensive —Agents Armstrong and Allen instructed Monteilh to "empty [his] head" about what he had learned that

day—so that Monteilh regularly spent an hour or two each evening writing notes. After a while, these notes became so voluminous that Armstrong and Allen instructed Monteilh to prepare separate "supplemental notes" containing any sensitive or particularly valuable information. These were all handwritten. Armstrong and Allen took these notes from Monteilh when they met him twice a week.

135. At times, Monteilh reported to Agents Armstrong and Allen that when he was left alone in a mosque office, he had looked in drawers for information. Armstrong and Allen never instructed him not to do this.

136. Agents Armstrong and Allen were well aware that many of the surveillance tools that they had given Monteilh were being used illegally. Agent Armstrong once told Monteilh that while warrants were needed to conduct most surveillance for criminal investigations, "National security is different. Kevin is God." Agent Armstrong also told Monteilh more than once that they did not always need warrants, and that even if they could not use the information in court because they did not have a warrant, it was still useful to have the information. He said that they could attribute the information to a confidential source if they needed to.

137. Over the course of the fourteen months that Agents Armstrong and Allen supervised Monteilh's work as an informant in the Los Angeles and Orange County Muslim communities, they gathered hundreds of phone numbers and thousands of email addresses of Muslims. They also obtained background information on hundreds of individuals, gathered hundreds of hours of video recordings that captured the interiors of mosques, homes, businesses, and the associations of hundreds of Mus-

lims. They also obtained thousands of hours of audio recording of conversations—both where Monteilh was and was not present—as well as recordings of public discussion groups, classes, and lectures occurring in mosques and at other Muslim religious and cultural events.

The FBI's Oversight, Supervision, and Use of Monteilh

138. Upon information and belief, FBI Agents Armstrong and Allen, as well as their superiors Director Tidwell, and Agents Walls and Rose, maintained extremely close oversight and supervision of Monteilh. Moreover, because they made extensive use of the results of his surveillance, they knew in great detail the nature and scope of the operation, including the methods of surveillance Monteilh used and the criteria used to decide his targets, and continually authorized their ongomg use.

139. From about August 2006 to October 2007, Agents Armstrong and Allen met with Monteilh about twice per week for meetings to discuss their assignments for him, to give him instructions, to obtain his daily notes, and to either exchange his recording devices for fresh ones or upload the recordings to a computer. These meetings were held in public places, outside the areas where the Muslim community lived. About once per month, they met with Monteilh in a room at the Anaheim Hilton Hotel, where they discussed the information he had obtained and gave him instructions in greater detail.

140. Agents Armstrong and Allen monitored and supervised Monteilh's work as an undercover informant closely. Through the daily notes they collected from him and the twice-weekly meetings, Monteilh told them about virtually everything he did and all the information he had obtained. They gave Monteilh instructions, or

"tasking orders," regularly. They gave him both standing instructions on kinds of information to gather whenever possible—for example, to meet and get contact information for a certain number of Muslims per day—and also gave him specific instructions on information they wanted, often in response to information he provided—such as, for example, instructions to get inside a certain house within the week or to have lunch with a particular person two times. Agents Armstrong and Allen also gave Monteilh standing orders to call one of them every day, even on his days off, which Monteilh would do, apprising them on the call of his day's activities.

141. Agents Armstrong and Allen at various times discussed with Monteilh what happened to these notes. They said that their supervisors read the notes, that the notes were seen in "the Beltway," that they were seen by people with "a lot of authority," and that the Assistant Director in Charge of the FBI's Los Angeles field office, who at that time was Stephen Tidwell, read all of Monteilh's daily notes.

142. During the course of the investigation, Agents Armstrong and Allen discussed with Monteilh how the information he collected was actually being used. They assured him that all the information he collected was retained, and that they discarded none of it. They also told him that the information was used to build files on individuals: that every person he contacted—whose phone number he got, who he emailed, who he identified through photographs—had an individual file in which the information he gathered was retained.

143. On about four different occasions, during the meetings between Agents Armstrong and Allen and

Monteilh at the hotel room, they showed him a huge photo array on a large board consisting of the photos of around two hundred Muslims from the Orange County/ Los Angeles area. Agents Armstrong and Allen used different sets of photographs for each of these meetings, so that Monteilh saw hundreds of photographs over the four meetings. They instructed him to arrange the photos from the most dangerous to the least based on his knowledge and experience. The entire leadership of the Islamic community were in the photos—sheikhs, imams, board members; prayer leaders, leaders of civic organizations, and youth groups. The process took hours. Agents Armstrong and Allen also asked Monteilh to assist them in organizing the photos according to categories such as financial, operative, and leadership; to divide photos into possible cells according to mosques and ethnicity or nationality. The first of these meetings was in about March 2007, and the last was in about September 2007.

144. Over the course of several conversations, Agents Armstrong and Allen told Monteilh that they considered the leaders in the Muslim community—board members and leadership at mosques and leaders of Muslim organizations—to be potential threats, and that they regularly surveilled them and maintained more detailed files of information on their background and activities.

145. In about early spring of 2007, Agents Armstrong and Allen told Monteilh that information he had provided was particularly valuable, and told him he was "gold" in Los Angeles and in Washington. Agent Allen said that information from the operation was followed by people "at the highest levels," and that the operation was among the ten most important intelligence investi-

gations going on in the country. In about March or April 2007, Agent Allen said that he had meetings with Stephen Tidwell and one of his supervisors from Washington, D.C., Joseph Billy, Jr., about the operation.[30] Around the same time period, Agent Allen flew to Washington, D.C. with his supervisor, Pat Rose, in part to meet with high-level FBI officials to get approval to open a gym for Muslims that would function in part as a mosque with a prayer room. Agent Allen told Monteilh that approval to open the gym had been granted.

146. At around that time, Agents Armstrong and Allen told Monteilh that information from the operation would be shared with other agencies—that information obtained on people's finances or foreign assets was shared with the Treasury Department, and that information about people's immigration issues would be sent to immigration officials.

The End of the Monteilh Operation

147. Agents Allen and Armstrong had instructed Monteilh to ask general questions about *jihad* from the beginning of the operation. In early 2007, they instructed him to start asking more pointedly about *jihad* and armed conflict, then to more openly suggest his own willingness to engage in violence. Pursuant to these instructions, in one-on-one conversations, Monteilh began asking people about violent *jihad*, expressing frustration over the oppression of Muslims around the world, pressing them for their views, and implying that he might be willing or able to take action.

---

[30] Upon information and belief, Billy was at the time the FBI's Assistant Director in Charge of the agency's Counterterrorism Division.

148. In about May 2007, on instructions from his handlers, Monteilh told a number of individuals that he believed it was his duty as a Muslim to take violent actions, and that he had access to weapons. Many members of the Muslim community at ICOI then reported these statements to community leaders, including Hussam Ayloush. Ayloush both called the FBI to report the statements and instructed the individuals who had heard the statements to report them to the Irvine Police Department, which they did.

149. As a community, ICOI also brought an action for a restraining order against Monteilh to bar him from the mosque. A California Superior Court granted the restraining order in June 2007.

150. After the court granted the restraining order, Monteilh continued going to other mosques for a month or two, but then disappeared from the Muslim community.

151. At around the same time—during the summer of 2007—Agents Armstrong and Allen told Monteilh that Defendant Barbara Walls, then the Assistant Special Agent in Charge of the FBI's Santa Ana office, had come to distrust him and did not want him working any more. They told him there was significant conflict between Agent Walls and field agents over how to handle the operation, and that there had been an audit team sent from Washington, D.C., to examine Agent Walls' handling of one of the leads from the operation. Because of this conflict and complications surrounding the restraining order, Agents Armstrong and Allen told Monteilh in about September 2007 that he would be going on hiatus from undercover work in the Orange County Muslim community.

152. During one of their final meetings with Monteilh in about October 2007, Agent Allen told Monteilh that although his role was over, Operation Flex and the FBI's operations in Orange County and Los Angeles would continue. He said that the information Monteilh had provided was a valuable foundation for the FBI's continuing work.

153. During one of the final meetings between Agents Armstrong and Allen and Monteilh, Agent Walls was also present. She warned Monteilh to stay silent about the operation.

154. In August 2008, Monteilh returned to Irvine and contacted the Irvine Police Department to voice concerns about his safety because of his role as an informant. He spoke with a detective, as well as a sergeant that he recognized as someone who had once escorted him when he was undercover with his handlers. The sergeant knew very specific information about individuals Monteilh had surveilled who he had concerns about, and told Monteilh in this meeting that he worked for JTTF. He told Monteilh that several individuals he had asked him about were still under surveillance. He also specifically mentioned that surveillance was ongoing at gyms and at least two mosques.

Monteilh's Identity Revealed

155. On or about about February 20, 2009, a man named Ahmed Niazi was arrested in Orange County and charged in federal criminal court with immigration fraud for lying on his naturalization application.

156. Niazi had met Monteilh at ICOI and had spent a significant amount of time with him. Niazi had heard Monteilh's most direct statements about *jihad* and had

reported those statements to Hussam Ayloush and to the Irvine Police Department.

157. At Niazi's bail hearing, which occurred on February 24, 2009 in federal district court in Santa Ana, California, FBI Special Agent Thomas Ropel testified that Niazi presented a threat to national security. Agent Ropel testified that he had heard numerous recordings of conversations between Niazi and a confidential informant. Agent Ropel stated that this confidential informant was the man Hussam Ayloush had reported to the FBI, and that Niazi and another individual had reported to the Irvine Police Department. Together, these statements confirmed that the informant was Craig Monteilh, and that he had recorded numerous conversations that he had while an informant.

158. Charges against Niazi were dismissed at the request of the United States Attorney's office on about September 30, 2010.

159. Agent Ropel's testimony on February 24, 2009 confirmed for the first time that Monteilh was a confidential informant for the FBI who had recorded numerous conversations.

160. Prior to that testimony, Plaintiffs did not know and could not reasonably have known that Monteilh was working for the FBI as an informant; that the FBI and Defendants, through Monteilh, had surveilled and gathered information about them from their interactions with Monteilh; and that the FBI had subjected them to this surveillance because of their religion. Upon information and belief, prior to February 2009, Monteilh never told anyone outside of law enforcement and his immediate family that he was working as an informant for the FBI.

161. Subsequent to Ropel's testimony, a number of different sources have confirmed that Monteilh worked for the FBI, including Monteilh himself.

162. In news accounts of the investigation, Monteilh himself has stated to reporters that the FBI paid him more than $170,000 over fifteen months to be an undercover informant in mosques in Orange County, that "he was instructed to infiltrate mosques throughout Orange [County] and two neighboring counties in Southern California," that he was "ordered to randomly surveil and spy on Muslims to ferret out potential terrorists," and that his handlers told him that "Islam is a threat to our national security."[31]

163. Upon information and belief, on August 20, 2007, the district attorney in a state criminal case against Monteilh from 2003 moved to terminate his probation early. In the proceeding, the district attorney explained the basis for the termination:

> Apparently, [Monteilh] is working with F.B.I. Agent Kevin Armstrong. He has given Agent Armstrong very, very valuable information that has proven to be essential in an F.B.I. prosecution. It was Agent Armstrong that contacted the head deputy and the head deputy instructed us to ask for termination.[32]

---

[31] *See* Jerry Markon, *Tension grows between Calif. Muslims, FBI after informant infiltrates mosque*, WASH. POST (Dec. 5, 2010).

[32] Transcript of Proceedings held Aug. 20, 2007, Probation Termination, *People v. Monteilh,* L.A. Sup. Ct. No. KA059040, filed in support of Motion to Set Aside Conviction, Exh. I, *Monteilh v. Federal Bureau of Investigation,* Dkt. 89-9, Case No. 10-cv-00102 JVS (RNBx) (C.D. Cal.).

A copy of the transcript is attached hereto as Attachment 1.

164. Further confirmation comes from court documents filed in a civil action that Monteilh brought against the FBI and the City of Irvine. In some of those documents, the City of Irvine acknowledged that while a pending criminal investigation of Monteilh was underway, members of the FBI's Orange County Joint Terrorism Task Force approached members of the Irvine police force and asked them to delay any action against Monteilh.[33]

165. In discovery served by Monteilh in that same federal lawsuit, the City of Irvine admitted that it and its agents "were aware that [Monteilh] was an FBI informant," and that the City of Irvine "[was] informed by the FBI that [Monteilh] was an FBI informant."[34]

166. Correspondence in connection with that lawsuit provides yet more evidence of Monteilh's work as an FBI informant. Upon information and belief, on June 16, 2010, Associate General Counsel for the FBI, Henry R. Felix, sent a letter to Adam Krolikowsi, an attorney representing Monteilh in his civil action against the FBI, in reply to a letter Krolikowski had sent the previous day. Felix's June 16 letter indicated that Monteilh had signed a non-disclosure agreement with the FBI on October 5, 2007. Felix noted that Krolikowsi had sent

---

[33] *See* Answer to Complaint of City of Irvine and Ronald Carr, *Monteilh v. Federal Bureau of Investigation,* Dkt. 23, Case No. 10-cv-00102 JVS (RNBx) (C.D. Cal.).

[34] *See* Motion to Set Aside Conviction, Exh. G, *Monteilh v. Federal Bureau of Investigation,* Dkt. 89-7, Case No. 10-cv-00102 JVS (RNBx) (C.D. Cal.) (exceprts [*sic*] of City of Irvine's responses to requests for admissions).

previous letters, but stated that his most recent letter mentioned "Operation Flex" and that this was "the first letter in which [Krolikowski] reference[d] a particular FBI operation or investigation." A copy of this letter is attached hereto as Attachment 2.[35]

167. Monteilh himself confirms many of the above-described details of his work as an informant, including that he worked for the FBI to infiltrate the Muslim community of Southern California from about July 2006 until October 2007; that, during this time, he spent about six or seven days a week posing as a Muslim convert named Farouk al-Aziz; that he conducted surveillance and other information-gathering on a wide variety of individuals and organizations in the Muslim community, solely because they were Muslim; and that he conducted surveillance of Plaintiffs as alleged below.

Monteilh's Interactions with Sheikh Yassir Fazaga

168. Agents Armstrong and Allen instructed Monteilh to conduct surveillance of the Orange County Islamic Foundation (OCIF) mosque in Mission Viejo, California. The imam of that mosque is Plaintiff Yassir Fazaga.

169. Agents Armstrong and Allen told Monteilh they believed that Plaintiff Fazaga, the imam of OCIF, was a radical, for several reasons: They said that Fazaga directed students on how to conduct demonstrations and encouraged them to speak out. They said that when the FBI Assistant Director in Charge of the Los Angeles Field Office, Stephen Tidwell, attended a meet-

---

[35] A copy of the letter was filed by Monteilh in his damages action against the FBI. *See* Motion to Set Aside Conviction, Exh. D, *Monteilh v. Federal Bureau of Investigation,* Dkt. 89-4, Case No. 10-cv-00102 JVS (RNBx) (C.D. Cal.).

ing at an Orange County mosque in about spring 2006, Fazaga openly pressed Tidwell about FBI informants in mosques, and when Tidwell denied putting informants in mosques, Fazaga had openly said he did not believe Tidwell. They also said that Fazaga was a person of interest because he was a board member of "In Focus News," a prominent Muslim newspaper that was vocal in speaking out against U.S. government actions that negatively affected Muslims and which Agents Armstrong and Allen believed was anti-American and linked to Muslim civil rights groups.[36]

170. Agents Armstrong and Allen told Monteilh that OCIF was linked to ICOI, a mosque they were also interested in, because the two mosques held joint events and jointly organized foreign trips, including the hajj pilgrimage to Mecca. They referred to OCIF as a "definite hotspot."

---

[36] Southern California *InFocus News* is the largest Muslim newspaper in California, with a circulation of about 25,000 and distribution at over 350 Muslim businesses and mosques throughout California, including every major mosque in Los Angeles and Orange County. According to its website, the paper's objective is to provide honest, effective and professional reporting, with a focus on California Muslims that both brings forth issues of concern to the California Muslim communities and provides a window into the American Muslim experience for all Californians. The paper has not only covered stories on local Muslim events and leaders, but has examined taboo topics such as domestic violence in the Muslim community and written stories to bridge community divides, such as by profiling families of other religions. Like many other newspapers, *InFocus News* has at times given news coverage or printed opinion pieces that supported or opposed various policies of the United States government. The paper has never advocated violence against the United States or its citizens or done anything else that would reasonably justify characterizing it as "anti-American."

171. Agents Armstrong and Allen also told Monteilh that OCIF was radical because it had certain religious scholars as guest speakers whom they believed were radical—particularly Yusef Estes, Suhaib Webb, and a local imam, Ahmad Sakr. They said that a moderate mosque would not have chosen these guest speakers.

172. Agents Armstrong and Allen instructed Monteilh to attend the Yusef Estes lecture which Sheikh Fazaga's mosque hosted. They equipped him with hidden video equipment that he used to video record the entire lecture, the literature Estes had set out, and the people who attended.

173. Pursuant to Agent Armstrong and Allen's instructions, Monteilh attended OCIF a number of times to conduct surveillance, including during Sheikh Fazaga's sermons.

174. Agent Armstrong and Allen also equipped Monteilh with a video camera hidden in a shirt button that he used to take video of the interior of OCIF. Agents Armstrong and Allen instructed Monteilh to get a sense of the schematics of the place—entrances, exits, rooms, bathrooms, locked doors, storage rooms, as well as security measures and whether any security guards were armed. Agent Armstrong later told Monteilh that they had used the information he gathered to enter the mosque.

175. On the instructions of Agents Armstrong and Allen, Monteilh made video recordings of an area in the back of OCIF where there were religious books available for congregants to use, so that they could determine if any of the literature there was extremist.

176. Agents Armstrong and Allen also instructed Monteilh to make contacts within Sheikh Fazaga's Mis-

sion Viejo congregation. To comply, Monteilh worked out on various different occasions with about 40 of their congregants, usually in groups, obtaining the email address and cell phone number of anyone he worked out with and passing that information on to his handlers.

177. Agents Armstrong and Allen instructed Monteilh to gather additional information on a few individuals within the congregation who seemed to have the most direct access to Fazaga—to gather their email addresses, cell phone numbers, and addresses, as well as basic background information such as their occupation, whether they were married or had children, and what prayers they attended. Monteilh gathered this information and passed it on to Armstrong and Allen.

178. Agents Armstrong and Allen instructed Monteilh to monitor Fazaga at the prayers he conducted, to record and report on what he said, to talk with him afterwards and see who else talked to him afterwards, and to note individuals who appeared to be close to him. Monteilh also monitored what was said by a member of the congregation who substituted for Fazaga during one of the prayers.

179. In about April 2007, a member of the community introduced Monteilh to Fazaga while he was recording with a hidden video camera. Monteilh also obtained Fazaga's cell phone number and email address (not through Fazaga, but through others) and passed those on to Agents Armstrong and Allen, who told him they used the email addresses and telephone numbers gathered to monitor communications and conduct further surveillance.

180. Monteilh also gave Agents Armstrong and Allen the license plate numbers of cars Fazaga traveled in and the people with whom Monteilh saw him associate.

181. Agents Armstrong and Allen instructed Monteilh that whenever he saw Fazaga at another mosque or anywhere outside OCIF, he should call them and let them know immediately. Monteilh did this at least once when he saw Fazaga at another mosque.

182. On one occasion, during Friday afternoon prayer at OCIF, the mosque had a booth set up to collect donations for some kind of relief for Muslims abroad. Pursuant to Agents Armstrong and Allen's orders to monitor donations, Monteilh stood near the booth and used the hidden video camera to make video recordings of people who went up to the booth to contribute money.

183. After Monteilh's role as an FBI informant became publicly known in 22 February 2009, many members of the OCIF congregation were horrified to learn that the man who spent so much time in their mosque was an informant. This revelation significantly undermined the trust within that community, which in turn deterred members from worshipping as a congregation.

184. Since he had contact with Monteilh, Fazaga has also been subjected to secondary screening and searches upon return to the U.S. from various international trips, being held between 45 minutes and three hours most times he travels.

185. Since discovering the FBI surveilled him and the mosque where he serves as imam, Sheikh Fazaga believes that any of his communications in the mosque and over telephones may be monitored, and indeed that he may be under surveillance at any time. As an intern

therapist as well as an imam, Fazaga provided counseling to congregants and Muslims at the mosque as part of his service to the Muslim community. Since learning of the FBI's surveillance, he no longer counsels congregants at the mosque for fear that their conversations are monitored and therefore the personal information shared is not confidential, which has limited his capacity to provide such counseling. The constant fear of being under surveillance, the scrutiny during travel, the effect on the sense of community at his mosque and others, and the additional difficult in providing counseling to clients have all caused Sheikh Fazaga severe and ongoing anxiety and emotional distress.

Monteilh's Interaction with Plaintiff Ali Uddin Malik

186. In their early meetings with Monteilh, Agents Armstrong and Allen showed Monteilh a picture of a young man who they identified as Plaintiff Ali Malik. They told him Malik had been a surfer kid in Newport Beach who wore dyed hair, but had travelled to Yemen to attend a religious school, and had returned to the U.S. wearing traditional Muslim dress and a full beard.

187. Agents Armstrong and Allen told Monteilh that Malik's change in behavior in embracing religion and traditional dress was highly suspicious and for that reason they needed to investigate him. They also told him they were suspicious of Malik because he was involved with people from the "MSU." ("MSU" stands for "Muslim Student Union," which is the name of Muslim student groups at many colleges and universities, including U.C. Irvine.) Agent Armstrong told Monteilh that before he was assigned to be his handler, he had been assigned to investigate the MSUs and young Muslims, including Ali Malik.

188. Agents Armstrong and Allen told Monteilh that the way that Malik groomed his beard indicated that he was a radical.

189. Agents Armstrong and Allen already had information on Malik and his family before they assigned Monteilh to do anything, but they told Monteilh to get more information on one of his brothers; on another individual who Malik was close to; on Malik's associations from the Irvine mosque, and on anyone with whom Malik hung out at the gym.

190. Agents Armstrong and Allen said that they knew Malik had been to an Islamic religious school in Yemen, and that he had been blocked from entering Saudi Arabia after he had traveled to Yemen. They tasked Monteilh with finding out what school he had been to and why he had been denied entry into Saudi Arabia. Upon information and belief, Armstrong and Allen already had knowledge of this information. When reentering the country in 2006, Malik had been interviewed at length by U.S. officials and had fully disclosed the nature of his travels, including his study at Dar al-Mustafa. Malik also disclosed that while abroad, he had traveled to Abu Dhabi in hopes of getting a visa to Saudi Arabia for Umrah (the minor pilgrimage in Islam). However, Malik was informed by individuals both at Dar al-Mustafa and in Abu Dhabi that he needed to apply for a visa with the Saudi embassy in the United States, which was logistically impossible to do during his trip, so that Malik did not attempt to enter Saudi Arabia or even apply for a visa during his 2006 trip.

191. In about April 2007, Agents Armstrong and Allen began discussing the possibility of sending Monteilh abroad to study Islam and Arabic. When Monteilh

started asking about a school to go to, Malik told him that he had attended Dar al-Mustafa in Tarim, in Yemen. Monteilh reported this information to Agents Armstrong and Allen.

192. On several occasions, Monteilh used the key fob or cell phone recording devices provided by Agents Armstrong and Allen to record groups of young Muslims talking in the prayer hall, particularly after *ishaa* prayer. On these occasions, Monteilh greeted people, left his things—including the recording device—near where they were talking, and then went to another part of the mosque (or a different part of the prayer hall) to pray so that the recording device would capture their conversation when he was gone. On several of these occasions, Ali Malik was one of the people in the group Monteilh recorded. Monteilh recorded these conversations when he was not present, then gave notes that detailed the people he saw there to Agents Armstrong and Allen, so they would be able to identify the voices. Agents Armstrong and Allen received notes in which Monteilh said that he had recorded these conversations without being physically present, and never told him not to do this.

193. The prayer hall of a mosque is sacred space where particular rules and expectations apply. Shoes are prohibited, one must be in a state of ablution, discussing worldly matters is discouraged, and the moral standards and codes of conduct are at their strongest. Gossiping, eavesdropping, or talebearing *(namima*—revealing anything where disclosure is resented) is forbidden. *Halaqas,* or small group meetings, are understood by attendees of the mosque to be safe environments in which to discuss theology or matters related to the practice of Islam, and that correspondingly ensure

some measure of confidentiality among participants. In addition, audio and video recording without permission were barred at ICOI, and on rare occasions where an outside entity recorded an event or speaker, signs notified congregants of the recording.

194. Malik more than once told Monteilh that he heard Monteilh was going regularly to *fajr,* or early morning prayer. Malik commended Monteilh on his commitment —he said that he had gotten into the routine of attending *fajr* prayers daily when he had been studying abroad, but that, regrettably, it was easy to fall into attending prayers only when it was convenient. He stated that he wanted to get back to that kind of regimen. Agents Armstrong and Allen told Monteilh this was significant information that indicated Malik was returning to extremist beliefs, which justified further surveillance.

195. Agents Armstrong and Allen received significant information on Malik. In addition to the surveillance described above, including recordings of all Monteilh's conversations with Malik, they several times showed Monteilh photos with people they said had seen with Malik and asked him to identify them. The pictures sometimes had Malik in them.

196. Since his contact with Monteilh, Malik has repeatedly been subjected to extended interviews with FBI and Customs upon re-entering the country, including one interview that lasted for several hours, resulted in him missing a connecting flight, and consequently missing a summer school class that made him lose credit for the class and required that he push his college graduation back by several months at considerable financial expense.

197. Also as a result of the FBI's surveillance, Malik altered his religious practices. Because he understood he was targeted because of his outwardly religious appearance, adherence to Islamic ritual practice, and involvement with the mosque and Muslim Student Union at UCI, Malik trimmed his beard, does not regularly wear a skull cap any longer, and stopped attending the mosque regularly for an extended period of time. To this day, he attends mosque less frequently than he did before having contact with Monteilh because of his fear of being monitored at mosque and the effect that this fear has on his sense of the mosque as a place of peace and spiritual refuge. This interference with his religious practice results from Defendants' actions and has caused Malik severe and ongoing anxiety and emotional distress.

198. Malik also believes his reputation in the community to have been damaged. He believes that because of his association with Monteilh, people have also assumed that he is a government informant and act as if they are suspicious of him. He believes that he does not have the full trust of the Muslim community. This belief that others suspect him because of Defendants' actions has caused Malik severe and ongoing anxiety and emotional distress.

199. Since discovering the FBI surveilled him and the mosque he attended, Malik believes that any of his communications in the mosque and over telephones may be monitored, and indeed that he may be under surveillance at any time. He curtails phone and email conversations with his friends and family because of his belief that they may be monitored. He also suspects that any newcomer to a mosque may be an FBI informant, and has refused to be as welcoming to newcomers as he believes

his religion requires. This constant fear of being under surveillance because of Defendants' acts has caused Malik severe and ongoing anxiety and emotional distress.

Monteilh's Interaction with Yasser AbdelRahim

200. A few weeks after Monteilh took *shahadah* at ICOI, a group of young men approached him at the mosque, said they were impressed that he attended mosque so regularly and invited him to socialize with them at their house. Agents Armstrong and Allen told Monteilh that the men's home was already under surveillance because it was shared by five young, unmarried Muslim Egyptian men with different skills and backgrounds—including a computer analyst, a pharmacist, an accountant, and one who handled logistics—and that for that reason they believed they might be a Muslim Brotherhood cell.

201. A few days after this invitation, Monteilh told Agents Armstrong and Allen that one of the young men who lived at the house, Plaintiff Yasser Abdel AbdelRahim, was a person who seemed to attract and have influence with young Muslims. Agents Armstrong and Allen told him they thought AbdelRahim was the leader of the cell, and that he should spend time at their house, and with AbdelRahim in particular, and gather as much information as he could. Monteilh did so, and gave recordings of all the conversations he had with AbdelRahim and the other members of the house to Agents Armstrong and Allen, along with notes about his observations.

202. Agents Armstrong and Allen told Monteilh to get into every room in AbdelRahim's house to see what was in there, and include that information in his reports. Later, in about February or March of 2007, Armstrong

and Allen equipped Monteilh with a video camera hidden in a shirt button and instructed him to conduct video surveillance of the layout and contents of the house, which he did.

203. Shortly after first meeting Monteilh, AbdelRahim and one of his roommates bought Monteilh some books on Islam, and later asked he what thought of them. Some time after that, AbdelRahim agreed to meet with Monteilh to teach him various prayers. Agents Armstrong and Allen expressed excitement at this, and asked for the first sheet of paper on which AbdelRahim had written a prayer for Monteilh to learn, telling him when they gave it back a few days later that they had lifted AbdelRahim's fingerprints from it.

204. When Monteilh reported that AbdelRahim always led prayer in the house, Agents Armstrong and Allen said that showed leadership, and confirmed that the surveillance should focus on him.

205. Pursuant to standing instructions from Agents Armstrong and Allen, Monteilh gathered and provided them information about AbdelRahim's travel plans, particularly when AbdelRahim was going to or from Egypt to see his family or his fiance's family. After one of these trips to Egypt, AbdelRahim complained that he had questioned for a long time when he re-entered the country—that he expected some delay but this had been way too long. Agents Armstrong and Allen told Monteilh they had been responsible for that questioning.

206. During this time, AbdelRahim played pick-up soccer with other Muslim youth. Monteilh attended some of these games and took down the license plates of people who attended. On more than one occasion, he made a video recording with a hidden camera Agents

Armstrong and Allen provided him, in order to document who was attending and socializing with one another.

207. After Monteilh learned through conversations that AbdelRahim traveled to a particular city for his job, Agents Armstrong and Allen had a particular group of Muslims in that city surveilled and believed he went there to report or get instructions from this group. As Agents Armstrong and Allen had told Monteilh to report all travel plans, he reported AbdelRahim's travel plans on several occasions. Agents Armstrong and Allen told Monteilh that they had AbdelRahim surveilled when he traveled, based on Monteilh's information.

208. Monteilh talked to AbdelRahim about his fiancée, who lived in Detroit, and her family, and transmitted what information he learned to Agents Armstrong and Allen—including her email address.

209. On different occasions, Agents Armstrong and Allen told Monteilh that the FBI had electronic listening devices in AbdelRahim's house, as well as in AbdelRahim's car and phone. For example, one day, one of Monteilh's handlers called to tell him that a friend had driven up to AbdelRahim's house quickly in an agitated state, and asked Monteilh to go down there to find out what was going on. When Monteilh asked how he knew this, he indicated they had video outside the house. Another time, Agents Armstrong and Allen asked him about something that happened inside the house that he hadn't yet put in his notes, then told him that they knew because they had audio surveillance in the home.

210. Agents Armstrong and Allen said that AbdelRahim was donating money to a charitable organization in Egypt and that these donations had been tracked by the Treasury Department. They said that these dona-

tions were not unlawful, but that they could make them seem suspicious in order to threaten him and pressure him to provide information and become an informant.

211. On many Tuesday nights, an imam from the Garden Grove mosque gave Arabic language teachings at ICOI. AbdelRahim often attended. On several occasions, Monteilh used recording devices provided by his handlers to record these teachings and the discussions afterward by going into the prayer hall to pray near the group, then leaving his things—including the recording device (disguised as a key fob or cell phone)—near to where the group was talking, and then go to another part of the mosque or a different part of the prayer hall to pray. The recording device would capture their conversation when Monteilh was not within earshot. AbdelRahim was part of the group when Monteilh recorded on several occasions.

212. On instructions from Agents Armstrong and Allen, Monteilh asked AbdelRahim questions about *jihad* and pressed him on his views about religious matters and certain religious scholars (particularly Egyptian ones) in order to get him to say something that might be incriminating or provide a way to pressure him to provide information to the FBI. AbdelRahim told Monteilh that there was more to Islam than *jihad*: that *jihad* is a personal struggle, and that to the extent that there is such thing as a fighting *jihad,* the Quran places very strict rules that prohibit harming plants or trees, infants, elderly or women, and that terrorists who say they are engaged in *jihad* are committing murder. When Monteilh brought up religious scholars Agents Armstrong and Allen had instructed him to mention, like Hassan al-Banna and Sayid Qutb, AbdelRahim said

that he did not agree with them, but thought that the Egyptian government should not have executed them.

213. When Monteilh was reported to the FBI by Muslim community members, AbdelRahim was contacted by FBI agents and met with them to offer information about Monteilh and his extremist rhetoric. Upon information and belief, one of these agents was Defendant Paul Allen.

214. A few months later, AbdelRahim unexpectedly met the same FBI agents, who were waiting for him outside the office of his chiropractor. He was surprised to see them there as he had scheduled an appointment with the chiropractor just an hour or so prior. They went to a coffee shop and showed him a search warrant and told him that his storage unit was being searched by the FBI. Two days later, they met again with AbdelRahim and asked him if he knew of any person engaged in any suspicious activity at the mosque or elsewhere. They asked AbdelRahim if he minded contacting the agents if he came across any information of anyone doing anything. AbdelRahim understood that they were asking him to be an informant, and he refused. The FBI agents asked not to mention the offer to anyone.

215. Since he had contact with Monteilh, AbdelRahim has also been subjected to extensive secondary questioning and searches most of the times he has returned to the U.S. from trips abroad. These interrogations and the fear that he will be subjected to them when he travels have caused AbdelRahim severe anxiety and emotional distress.

216. Since discovering the FBI surveilled him and the mosque he attended, AbdelRahim believes that any of his communications in the mosque and over tele-

phones or email may be monitored, and indeed that he may be under surveillance at any time. He also suspects that any newcomer to a mosque may be an FBI informant, and has refused to be as welcoming to newcomers as he believes his religion requires. This constant fear of being under surveillance because of Defendants' acts has caused AbdelRahim severe and ongoing anxiety and emotional distress.

217. Since these incidents, AbdelRahim's confidence in the mosque as a sanctuary has been ruined. He significantly decreased his attendance to mosque services for fear of surveillance, and as such his donations to mosque institutions also decreased. This interference with his religious practice has caused AbdelRahim severe and ongoing anxiety and emotional distress.

CLASS ALLEGATIONS

218. Plaintiffs, as class representatives, bring claims for injunctive relief on behalf of themselves and all similarly situated persons pursuant to Rule 23(a) and (b)(2).

219. Plaintiffs, as class representatives, bring this action on their own behalf and on behalf of the following class:

> All individuals targeted by Defendants for surveillance or information-gathering through Monteilh and Operation Flex, on account of their religion, and about whom the FBI thereby gathered personally identifiable information.

220. *Numerosity.* The size of the class makes a class action both necessary and efficient. Plaintiffs estimate that the class consist of hundreds if not thousands of current and former residents of Southern California. Members of the class are ascertainable through a review

of Defendants' files on Operation Flex, but so numerous that joinder is impracticable.

221. *Typicality.* The claims of the Plaintiffs are typical of the claims of the class as a whole. Each of the Plaintiffs was subjected to surveillance by Defendants during the relevant period. As a result of Defendants' practices, Defendants have discriminated against each of Plaintiffs on the basis of their religion and religious practices, in violation of law. The unlawful policies and practices that have operated to discriminate against the Plaintiffs are typical of the unlawful practices that operated to discriminate against other class members so as to unlawfully target them for surveillance because of their religion and religious practices.

222. *Common Questions of Law and Fact.* This case poses common questions of law and fact affecting the rights of all members of the class, including, but not limited to:

a. Whether Defendants engaged in a program of conducting surveillance of mosques in Orange County, and the Plaintiffs and class members who attended those mosques;

b. Whether Defendants targeted Plaintiffs and class members for surveillance through Monteilh because they were Muslims or because of their practice of Islam;

c. Whether Defendants' practice of targeting Plaintiffs and class members for surveillance because they were Muslim or because of their practice of Islam constitutes impermissible religious discrimination under the First Amendment;

d. Whether Defendants' practice of targeting Plaintiffs and class members for surveillance because they were Muslim or because of their practice of Islam violates the guarantee of equal protection of the laws under the Fifth Amendment;

e. Whether Defendants' practice of targeting Plaintiffs and class members for surveillance because they were Muslim or because of their practice of Islam places a substantial burden on the religious exercise of Plaintiffs and class members under the First Amendment;

f. Whether Defendant FBI maintains records on Plaintiffs and class members, arising out of the investigation at issue, describing how they exercise rights guaranteed by the First Amendment;

g. Whether the maintenance by Defendant FBI of records on Plaintiffs and class members describing how they exercise rights guaranteed by the First Amendment is pertinent to and within the scope of lawful, authorized law enforcement activity;

h. Whether information gathered by Defendants pursuant to unlawful surveillance should be disgorged and purged from their files;

i. Whether Defendants conspired for the purpose of depriving Plaintiffs and other class members of their rights for purposes of 42 U.S.C. § 1985;

j. Whether and what kinds of declaratory and injunctive relief are appropriate.

223. *Adequacy of Class Representation.* Plaintiffs can adequately and fairly represent the interests of the class as defined above, because their individual interests

are consistent with, and not antagonistic to, the interests of the class.

224. *Adequacy of Counsel for the Class.* Counsel for Plaintiffs possess the requisite resources and ability to prosecute this case as a class action and are experienced civil rights attorneys who have successfully litigated other cases involving similar issues.

225. *Propriety of Class Action Mechanism.* Class certification is appropriate because the prosecution of separate actions against Defendants by individual class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants and because Defendants have acted or refused to act on grounds that apply generally to the class.

CLAIMS FOR RELIEF

First Cause of Action

Violation of the First Amendment Establishment Clause Claim under *Bivens*; 28 U.S.C. § 1331 (Against All Defendants except the FBI and United States by all Plaintiffs.)[37]

226. Plaintiffs incorporate Paragraphs 1-225 as if fully set forth herein.

227. As set forth above, Defendants engaged in a scheme to target Plaintiffs for surveillance because of Plaintiffs' adherence to and practice of the religion of Islam. This scheme discriminates against Muslims, in

[37] Plaintiffs' claims for damages under *Bivens* are made against those Defendants named in their individual capacities, while their claims for injunctive relief under Section 1331 are made against Defendants named in their official capacities.

violation of the Establishment Clause of the First Amendment to the United States Constitution.

Second Cause of Action

Violation of the First Amendment Establishment Clause Claim under 42 U.S.C. § 1985(3); 28 U.S.C. § 1343 (Against Individual Capacity Defendants by all Plaintiffs.)

228. Plaintiffs incorporate Paragraphs 1-227 as if fully set forth herein.

229. As set forth above, Defendants engaged in a scheme to target Plaintiffs for surveillance because of Plaintiffs' adherence to and practice of the religion of Islam and for the purpose of discriminating against Plaintiffs, as Muslims, in violation of the Establishment Clause of the First Amendment to the United States Constitution.

230. Through their scheme, Defendants conspired, and conspired to go in disguise on the premises of another, for the purpose of depriving Plaintiffs, directly or indirectly, of the equal protection of the laws, and of equal privileges and immunities under the laws, because of their adherence to and practice of Islam. Defendants performed these acts with discriminatory animus against Muslims.

Third Cause of Action

Violation of the First Amendment Free Exercise Clause Claim under *Bivens*; 28 U.S.C. § 1331 (Against All Defendants except the FBI and United States by all Plaintiffs.)

231. Plaintiffs incorporate Paragraphs 1-230 as if fully set forth herein.

232. As set forth above, Defendants engaged in a scheme to target Plaintiffs for surveillance because of Plaintiffs' adherence to and practice of the religion of Islam. This scheme discriminates against Muslims, in violation of the Free Exercise Clause of the First Amendment to the United States Constitution.

233. As set forth above, Defendants' surveillance placed a substantial burden on Plaintiffs' religious exercise in their practice of Islam and is justified by no legitimate government interest.

Fourth Cause of Action

Violation of the First Amendment Free Exercise Clause Claim under 42 U.S.C. § 1985(3); 28 U.S.C. § 1343 (Against Individual Capacity Defendants by all Plaintiffs.)

234. Plaintiffs incorporate Paragraphs 1-233 as if fully set forth herein.

235. As set forth above, Defendants engaged in a scheme to target Plaintiffs for surveillance because of Plaintiffs' adherence to and practice of the religion of Islam and for the purpose of discriminating against Plaintiffs, as Muslims in violation of the Free Exercise Clause of the First Amendment to the United States Constitution.

236. As set forth above, Defendants' surveillance placed a substantial burden on Plaintiffs' religious exercise in their practice of Islam and is justified by no legitimate government interest.

237. Defendants have conspired, and conspired to go in disguise on the premises of another, for the purpose of depriving Plaintiffs, directly or indirectly, of the

equal protection of the laws, and of equal privileges and immunities under the laws, because of their adherence to and practice of Islam. Defendants performed these acts with discriminatory animus against Muslims.

Fifth Cause of Action

Violation of Religious Freedom Restoration Act, 42 U.S.C. § 2000bb-1
(Against All Defendants by all Plaintiffs.)

238. Plaintiffs incorporate Paragraphs 1-237 as if fully set forth herein.

239. The actions of Defendants substantially burdened Plaintiffs' exercise of religion, and are neither in furtherance of a compelling governmental interest nor the least restrictive means of furthering any compelling governmental interest.

Sixth Cause of Action

Violation of Fifth Amendment Equal Protection Clause Claim under *Bivens*; 28 U.S.C. § 1331
(Against All Defendants except the FBI and United States by all Plaintiffs.)

240. Plaintiffs incorporate Paragraphs 1-239 as if fully set forth herein.

241. As set forth above, Defendants have engaged in a scheme to target Plaintiffs for surveillance because of Plaintiffs' adherence to and practice of the religion of Islam. This scheme discriminates against Muslims, in violation of the Equal Protection Clause of the Fifth Amendment to the United States Constitution.

Seventh Cause of Action

Violation of the Equal Protection Clause Claim under 42 U.S.C. § 1985(3); 28 U.S.C. § 1343 (Against Individual Capacity Defendants by all Plaintiffs.)

242. Plaintiffs incorporate Paragraphs 1-241 as if fully set forth herein.

243. As set forth above, Defendants have engaged in a scheme to target Plaintiffs for surveillance because of Plaintiffs' adherence to and practice of the religion of Islam. This scheme discriminates against Muslims, in violation of the Equal Protection Clause of the Fifth Amendment to the United States Constitution.

244. Defendants have conspired, and conspired to go in disguise on the premises of another, for the purpose of depriving Plaintiffs, directly or indirectly, of the equal protection of the laws, and of equal privileges and immunities under the laws, because of their adherence to and practice of Islam. Defendants performed these acts with discriminatory animus against Muslims.

Eighth Cause of Action

Violation of the Privacy Act, 5 U.S.C. § 552a(a)-(l) (Against Defendant FBI by all Plaintiffs.)

245. Plaintiffs incorporate Paragraphs 1-244 as if fully set forth herein.

246. Defendant FBI, through Monteilh, collected and maintained records describing how Plaintiffs exercised their First Amendment rights, in violation of 5 U.S.C. § 552a(e)(7). Collection and maintenance of these records is not expressly authorized by statute, not autho-

rized by Plaintiffs, and is neither pertinent to nor within the scope of an authorized law enforcement activity.

247. Defendant FBI's collection and maintenance of records of Plaintiffs' First Amendment activities was intentional and willful, insofar as Defendants gathered the information for the purpose of collecting and maintaining records of Plaintiffs' First Amendment activities.

248. On or about September 6 and 12, 2011, Plaintiffs submitted letters to the FBI requesting that the FBI disclose all records in the possession of the FBI, associated with each Plaintiff, that were "gathered through the surveillance of former FBI informant Craig Monteilh and/or Operation Flex, as well as any information derived from that information." The letters also requested that the FBI "expunge all records associated with [Plaintiffs] that describe the exercise of [their] rights under the First Amendment of the United States Constitution that were gathered through the surveillance of former FBI informant Craig Monteilh and/ or Operation Flex, as well as any records derived from that information." The FBI has to date failed to provide Plaintiffs with those records or otherwise to respond to their requests.

249. Defendant FBI has failed to disclose records as required by Section 552a(d)(1). The records requested are not exempt from disclosure pursuant to Section 552a(j-k) or any other applicable law.

Ninth Cause of Action

Violation of the Fourth Amendment Claim under *Bivens;* 28 U.S.C. § 1331. (Against All Defendants except the FBI and United States by all Plaintiffs.)

250. Plaintiffs incorporate Paragraphs 1-249 as if fully set forth herein.

251. Defendants' actions as set forth above constitute unreasonable searches in violation of the Fourth Amendment to the United States Constitution, including but not limited to Defendants' actions in audio recording Plaintiffs' communications without a warrant and where no party to the communication consented to the recording; video recording in homes and other places where Plaintiffs had a reasonable expectation of privacy against video recording; and entering and planting electronic listening devices in mosques without a warrant.

Tenth Cause of Action

Violation of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810 (Against All Defendants by all Plaintiffs.)

252. Plaintiffs incorporate Paragraphs 1-251 as if fully set forth herein.

253. Defendants, under color of law, acting through Monteilh, used electronic, mechanical, and/or other surveillance devices, without a warrant, to monitor Plaintiffs and their communications and/or activities, and to acquire information under circumstances in which Plaintiffs had a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

Eleventh Cause of Action

Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2671 *et seq.*
(Against Defendant United States by all Plaintiffs.)

254. Plaintiffs incorporate Paragraphs 1-253 as if fully set forth herein.

255. At all times relevant to the complaint, Defendants Armstrong, Allen, Rose, Tidwell and Walls, were employees of the United States, acting in the scope of their employment through their own actions and their directions to employees and agents, under circumstances that would render the United States, if a private person, liable for damages that their actions caused Plaintiffs under California law. The United States is therefore liable to Plaintiffs, as follows, pursuant to 28 U.S.C. §§ 1346(b) and 2674.

256. The United States, if a private person, would be liable to Plaintiffs for invasion of privacy under California law. Defendants' acts in conducting audio and video surveillance of Plaintiffs, through Monteilh and Operation Flex, in situations in which Plaintiffs' had a reasonable expectation of privacy, constitute intrusions into a private place or matter in a manner highly offensive to a reasonable person.

257. The United States, if a private person, would be liable to Plaintiffs for violations of the California constitutional right of privacy set forth in Article 1, section 1 of the California constitution. Defendants' conduct in conducting audio and video surveillance of Plaintiffs, both through Monteilh and Operation Flex, in situations in which Plaintiffs' had a reasonable expectation of privacy, and in compiling and maintaining information on Plaintiffs based solely on their religion and religious

practice, amounts to a serious invasion of their rights to privacy.

258. The United States, if a private person, would be liable to Plaintiffs for violations of California Civil Code section 52.1. By subjecting Plaintiffs to constant surveillance because of their religion, then publicly revealing that surveillance, Defendants have interfered, or attempted to interfere, by threats, intimidation, or coercion with the exercise or enjoyment by Plaintiffs of their rights to practice their religion and to be free from religious discrimination under the California Constitution, in violation of California Civil Code § 52.1.

259. The United States, if a private person, would be liable to Plaintiffs for the intentional infliction of emotional distress under California law. Defendants' acts constitute extreme and outrageous conduct, in which they engaged with the intention of causing, or a reckless disregard for the probability of causing, emotional distress in plaintiffs; which was the actual or proximate cause of severe or extreme emotional distress that Plaintiffs have suffered.

260. Plaintiffs presented the FBI with notification of the above-alleged incidents and claims for monetary damages in claims sent to the FBI using Standard Form 95 on or about February 21, 2011. The FBI failed to make any response to Plaintiffs' claims within six months after they were filed.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully request that the Court grant the following relief:

a. Certify a Class under Rule 23(b)(2), as described above;

b. Injunctive relief on behalf of Plaintiffs and all other putative class members ordering Defendants to destroy or return any information gathered through the unlawful surveillance program by Monteilh and/or Operation Flex described above, and any information derived from that unlawfully obtained information, as well as to comply with their obligations under the Privacy Act, 5 U.S.C. § 552a;

c. Compensatory and punitive damages for violations of the laws of the United States and California, in an amount to be proven at trial;

d. Liquidated damages in an amount to be proven at trial pursuant to 50 U.S.C. §§ 1810(a), 1828(a), and California Civil Code §§ 52(a), 52.1(b);

e. Reasonable attorneys' fees and costs;

f. Any other relief as this Court deems proper and just.

Dated: September 13, 2011

Respectfully Submitted,

ACLU FOUNDATION OF SOUTHERN CALIFORNIA

COUNCIL ON AMERICAN-ISLAMIC RELATIONS, CALIFORNIA

HADSELL STORMER KEENY RICHARDSON & RENNICK LLP

By: /s/ PETER BIBRING
PETER BIBRING

Attorneys for Plaintiffs

ATTACHMENT 1

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF LOS ANGELES—WEST COVINA BRANCH

No. KA059040

THE PEOPLE OF THE STATE OF CALIFORNIA,
PLAINTIFF

v.

CRAIG F. MONTEILH, DEFENDANT

West Covina, California; Aug. 20, 2008
2:40 P.M.

PROBATION TERMINATION

---

[1]

UPON THE ABOVE DATE, THE DEFENDANT NOT BEING PRESENT IN COURT AND NOT REPRESENTED BY COUNSEL; THE PEOPLE BEING REPRESENTED BY LINDA CHILSTROM, DEPUTY DISTRICT ATTORNEY OF LOS ANGELES COUNTY, THE FOLLOWING PROCEEDINGS WERE HELD:

[2]

CASE NUMBER:	KA059040
CASE NAME:	PEOPLE OF THE STATE OF CALIFORNIA VS. CRAIG MONTEILH
WEST COVINA, CALIFORNIA	AUGUST 20, 2007

DEPARTMENT NO. 8	HON. ABRAHAM KHAN, JUDGE
REPORTER:	DIANA WHITESEL, CSR NO. 6287
TIME:	2:40 P.M.

APPEARANCES:

(LINDA CHILSTROM, DEPUTY DISTRTICT ATTORNEY OF LOS ANGELES COUNTY.)

-oOo-

THE CLERK: PEOPLE ARE GOING TO MOVE TO MAKE A MOTION TO TERMINATE PROBATION.

THE COURT: CRAIG F. MONTEILH. KA059040.

MS. CHILSTROM: YOUR HONOR, I HAVE BEEN INFORMED BY MR. SATO OF MY OFFICE THAT HEAD DEPUTY SCOTT CARBAUGH HAS REQUESTED THAT THIS CASE—THAT THE PROBATION IN THIS MATTER BE TERMINATED.

THE COURT: CAN YOU GIVE ME A REASON?

MS. CHILSTROM: I DON'T KNOW A REASON. I WAS JUST TOLD IT WAS UPON THE REQUEST OF THE HEAD DEPUTY.

THE COURT: I'M GOING TO CONTINUE THIS UNTIL TOMORROW UNTIL YOU CAN GIVE ME A REASON. I USUALLY DON'T TERMINATE PROBATION UNLESS THERE IS SOMETHING I CAN RELY ON.

MS. CHILSTROM: NOT A PROBLEM.

I TAKE IT, WE'RE WAITING FOR MR. LINDARS.

MAY I MAKE A QUICK CALL?

[3]

(PAUSE IN PROCEEDINGS)

MS. CHILSTROM: YOUR HONOR, COULD THE COURT RECALL THE LAST CASE?

THE COURT: OKAY. WE'RE STILL ON THE RECORD IN CRAIG F. MONTEILH.

MS. CHILSTROM: YOUR HONOR, I JUST SPOKE WITH MR. SATO. INITIALLY I WAS JUST TOLD THAT THE HEAD DEPUTY WANTED THE PROBATION TERMINATED.

APPARENTLY THE DEFENDANT IS WORKING WITH F.B.I. AGENT KEVIN ARMSTRONG. HE HAS GIVEN AGENT ARMSTRONG VERY, VERY VALUABLE INFORMATION THAT HAS PROVEN TO BE ESSENTIAL IN AN F.B.I. PROSECUTION. IT WAS AGENT ARMSTRONG THAT CONTACTED THE HEAD DEPUTY AND THE HEAD DEPUTY INSTRUCTED US TO ASK FOR TERMINATION.

THE COURT: WELL, OKAY. I KNOW THE DEFENDANT HIMSELF WAS HERE IN APRIL AND HAD REQUESTED EARLY TERMINATION. AND I BELIEVE ON RECOMMENDATION OF THE DISTRICT ATTORNEY, I DENIED HIS REQUEST. AND THAT WAS BACK IN APRIL. THAT'S WHY I WANTED TO FIND OUT WHAT THE REASONS WHY WERE AT THIS TIME BECAUSE IT'S ONLY BEEN FOUR MONTHS AFTER.

BUT OTHERWISE HE'S PAID HIS FINANCIAL OBLIGATION AND HE'S OTHERWISE BEEN ON PROBATION—HOW LONG HAS HE BEEN ON? IT'S KA059040. IS THAT '03?

MS. CHILSTROM: IT IS '03, YOUR HONOR.

THE CLERK: YES, YOUR HONOR, SINCE MAY 5, '03.

THE COURT: ALL RIGHT. APPARENTLY HE'S HAD PROBATION EXTENDED. IT MAY HAVE BEEN BECAUSE OF A WARRANT THAT HAD BEEN ISSUED WHICH IT WOULD OTHERWISE TOLL THE RUNNING OF HIS PERIOD.

[3]

I'LL GRANT THE REQUEST FOR THE REAONS STATED.

MS. CHILSTROM: THANK YOU

(THE PROCEEDINGS IN THE ABOVE ENTITLED MATTER WERE ADJOURNED.)

-oOo-

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES—
WEST COVINA BRANCH

No. KA059040

THE PEOPLE OF THE STATE OF CALIFORNIA,
PLAINTIFF

v.

CRAIG F. MONTEILH, DEFENDANT

DATED: Dec. 2, 2009

REPORTER'S CERTIFICATE

DEPARTMENT 8 HON. ABRAHAM KHAN, JUDGE

I, DIANA WHITESEL, CSR NO. 6287, OFFICIAL REPORTER OF THE SUPERIOR COURT OF THE STATE OF CALIFORNIA, FOR THE COUNTY OF LOS ANGELES, DO HEREBY CERTIFY THAT THE FOREGOING IS A TRUE AND CORRECT TRANSCRIPT OF ALL OF THE ADMONITIONS TAKEN AT THE TIME OF THE TAKING OF THE PLEA AND PRONOUNCEMENT OF SENTENCE IN THE ABOVE-ENTITLED CAUSE; AND FURTHER THAT THE VIEWS AND RECOMMENDATIONS OF THE COURT, IF ANY, ARE CONTAINED THEREIN PURSUANT TO SECTION 1203.01 OF THE PENAL CODE THE ABOVE-ENTITLED MATTER.

/s/ DIANA WHITESEL, CSR NO. 6287
DIANA WHITESEL, OFFICIAL REPORTER

ATTACHMENT 2

U.S. Department of Justice
Federal Bureau of Investigation

Washington, D.C. 20535-0001

June 16, 2010

Adam J. Krolikowski, Esq.
Woods & Krolikowski
1200 Main Street, Suite H
Irvine, CA 92614

RE: Craig Monteilh [Confidential Communication]
Compliance with NDA Notice Requirement

Dear Mr. Krolikowski:

This office is in receipt of your letter to Steven Kramer dated June 15, 2010. In your letter you state that Mr. Montielh has "been asked to review and sign declarations prepared by the ACLU for a lawsuit they will be filing concerning civil rights violations by the FBI within the Islamic Community during the time period of Operation Flex." I am aware that you have sent previous letters to the FBI concerning the Non-Disclosure Agreement that Mr. Monteilh signed on October 5, 2007, however; this is the first letter in which you reference a particular FBI operation or investigation. In advance of June 17, 2010, please provide us with any information that you intend to include in these declarations that is/or may be covered by the Non-Disclosure Agreement. The FBI maintains that all the obligations created under the Non-Disclosure Agreement remain in effect. Notifica-

tion by Mr. Monteilh that he intends to disclose information covered by this agreement does not limit or nullify the obligations that he accepted by signing this agreement.

Sincerely,

/s/ HENRY R. FELIX

HENRY R. FELIX
Associate General Counsel
Civil Litigation Unit II
Office of the General Counsel
Federal Bureau of Investigation
PA 400
935 Pennsylvania Ave., NW
Washington, D.C, 20535
Phone: 202-220-9328
Fax: 202-220-9355

APPENDIX H

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

Case No.: SA CV 11-00301 CJC (VBKx)

YASSIR FAZAGA, ET AL., PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL., DEFENDANTS

Filed: Dec. 23, 2011

DECLARATIONS OF CRAIG MONTEILH SUBMITTED BY PLAINTIFFS IN SUPPORT OF THEIR OPPOSITIONS TO MOTIONS TO DISMISS

INDEX OF DECLARATIONS

DECLARATION OF CRAIG F. MONTEILH

I, Craig F. Monteilh, make this declaration of my own personal knowledge and if called to testify, I could and would do so as follows:

1. From about July 2006 until October 2007, I worked for the United States Federal Bureau of Investigation ("FBI") as an undercover informant assigned to infiltrate the Muslim community in Southern California. During this time, I spent about six or seven days a week posing as a Muslim convert named Farouk al-Aziz, conducting surveillance and gathering information on a wide variety of individuals and organizations in the Muslim community.

Background, Training, and Placement as an Undercover Informant

2. In around early 2004, I met some police officers in Orange County who were working on a FBI narcotics task force, and discovered that I knew information from time I had spent in prison that was relevant to some of their investigations. I began working for the task force as a confidential informant, under the supervision of an FBI agent assigned to the task force, Special Agent Christopher Gicking, and his supervisor, Special Agent Tracy Hanlon, who worked in the FBI's criminal division in Santa Ana. Over the next two years, I continued to work for the FBI, supervised by Agents Gicking and Hanlon, on a series of assignments as an undercover informant on different criminal enterprises.

3. In about May 2006, Agents Hanlon and Gicking asked if I wanted to work in a new type of assignment for the national security division of the FBI, investigating potential terrorists and infiltrating mosques. I said

I was interested and they arranged a meeting in or around June 2006 with FBI Special Agent Kevin Armstrong and another FBI agent, also named Kevin. They told me they worked for the FBI's counterterrorism division in Santa Ana, California, and were assigned to the Orange County Joint Terrorism Task Force ("JTTF"). Agent Armstrong told me that the head of their team, FBI Special Agent Paul Allen, was in Washington, D.C., but wanted to meet with me the following week. Agent Armstrong told me I would no longer be working with criminal division, but would work for counterterrorism from then on and that he and Agent Allen would be assigned to supervise and direct my work, or to be my "handlers." (References to "my handlers" here mean Agents Armstrong and Allen.)

4. The next week I met with Agent Armstrong and Agent Allen, who showed me FBI credentials and identified himself as the head of a counterterrorism team at the JTTF. During this meeting, we discussed my physical appearance and skin tone, and Agents Allen and Armstrong suggested that I could pass as Syrian or Algerian. I had another meeting with Agents Armstrong and Allen, just a few days later, where Agent Allen asked me various questions about my background and knowledge of politics and world affairs, which I understood was to gauge my suitability to work as an informant.

5. When Agents Armstrong and Allen hired me to work for the counterterrorism division, the FBI increased my pay from the $3,000 to $4,000 per month I made working for the criminal division to about $6,000 per month. Over the course of the next fourteen months, the FBI, through my handlers, increased my compensa-

tion as I became more accepted by the Muslim community and more useful as an informant, so that my compensation topped out at about $11,200 per month.

6. Eventually, my handlers told me that the FBI used the name "Operation Flex" for the surveillance program that used me. My handlers told me this repeatedly, and I heard other agents refer to it as well. My handlers told me that this was a reference to me, since I conducted informant work in gyms under the cover of working as a fitness consultant, both when I worked for the criminal division and for counterterrorism. But my handlers told me that Operation Flex was a broader surveillance program that went beyond just my work.

7. In about July 2006, my FBI handlers put me through a training program in which they had me learn the basics of the Arabic language and the religion of Islam. They explained that the purpose of this training was to make the account of my background more credible. Agent Armstrong also trained me in the martial art of Krav Maga. My handlers also talked to me extensively about how, once I began my assignment, I should progress in exhibiting the culture and customs of Islam. This training lasted approximately two weeks of twelve to fourteen hour days, with little time off, and took place in a large warehouse that my handlers drove me to while I was blindfolded. Agents Armstrong and Allen supervised the training.

8. In about late July 2006, my handlers told me to make an appointment to see Sheikh Sadullah Khan, an imam at the Islamic Center of Irvine ("ICOI"), a mosque in Irvine, California. My handlers told me to tell Khan that I was of Syrian and French descent and that I wanted to embrace my Islamic roots and formally con-

vert to Islam. My handlers gave me no background on Khan, but just told me to stick to this story. I made the appointment and then met with Khan a few days later in his office at ICOI, in the presence of two imams from mosques in Garden Grove and Anaheim. After a conversation with Khan, he told me I could take *shahaddah* (make a public declaration of my faith) the next day at the *jummah* prayer (the Friday prayer that is the most important service of the week). I reported this to Agent Allen and he instructed me to do so, so I came back to ICOI the next day and took *shahaddah* before a congregation of hundreds of Muslims. I immediately began to attend the mosque on a daily basis.

9. About a week after I took *shahaddah*, I took the Muslim name Farouk al-Aziz. I attended prayers daily, often multiple times a day. At first I attended prayers only at ICOI, but as time went on, my handlers encouraged me to go to other mosques around the area as well. Muslims who met me in the mosque generally embraced me as a new convert. On my handlers' instructions, I took every opportunity to meet people, get their contact information, meet them privately to get to know them, find out their background, find out their religious and political views, and get any information on them I could for the FBI.

10. My handlers told me that because of my criminal background, any information I collected would have to be recorded. My handlers told me, "If it isn't recorded, it didn't happen." My handlers initially gave me a small audio recording device called an "f-bird," but in about September 2006 replaced that with a cell phone and two key fobs (which looked like remote controls for car locks) with audio recording devices in them that could

be used to record conversations that went on around me. I used these recording devices to record all day, every moment I worked undercover, regardless who I was meeting or what was discussed. I would turn on one of the devices in the car before I left my house, and not turn it off until I arrived home. My handlers instructed me to record everything, without any limitations. Agent Allen told me later on that there was a team transcribing all the conversations I recorded, and although I frequently discussed recordings with my handlers, they never stated or even suggested that they attempted to minimize intrusions by listening only to snippets of conversations to see if they were relevant.

11. Beginning in about February 2007, on various occasions, my handlers outfitted me with video surveillance equipment that recorded through a camera hidden in a button in the front of my shirt. They told me that the video surveillance equipment also recorded audio. In the beginning, the video equipment was somewhat difficult to set up, and required my handlers' assistance, so I did not use it regularly. By about April 2007, my handlers had improved the design of the video equipment and I would use video surveillance several days per week. My handlers instructed me to use the video camera for various specific purposes to capture the internal layout of mosques, to film basketball or soccer games to see who associated with whom, to film guest lectures to see what was said and who attended, or when I went into people's houses. My handlers would also instruct me to go open particular doors in homes or mosques and film the room behind.

12. On my handlers' instructions, I also composed daily notes of my activities and the surveillance I had

undertaken. These notes were extensive—my handlers instructed me to "empty my head" about what I had learned that day—so that I regularly spent an hour or two each evening writing my notes. After a while, these notes became voluminous, and my handlers instructed me to prepare separate "supplemental notes" containing any sensitive or particularly valuable information. These were all handwritten. I gave them to my handlers when I met them twice a week.

13. Over the course of my work for the FBI, my handlers at various times discussed with me what happened to these notes. Agent Armstrong once told me that these notes were used as part of packages to obtain warrants for further surveillance on the individuals or organizations about whom I wrote. Both handlers talked to me at various times about federal judges reading my notes. My handlers also told me that their supervisors were reading the notes: Agent Allen once told me that my notes were seen in "the Beltway," that they were seen by people with "a lot of authority," and that the Assistant Director in Charge in the FBI's Los Angeles field office, who at that time was Stephen Tidwell, read all my notes.

14. From about August 2006 to October 2007, I met with Agents Allen and Armstrong about twice per week for meetings to discuss my assignments, for me to read through my notes with them so they could ask further questions, for them to give me instructions based on the information I provided, so I could give them my daily notes, and so they could either exchange my recording devices for fresh ones or upload the recordings to a computer while we spoke. These meetings were held in public places, outside the areas where the Muslim commu-

nity lived. About once per month, I met with my handlers in a room at the Anaheim Hilton Hotel, where they questioned me on the information I provided and gave me instructions in greater detail. I would also receive my payment at these monthly meetings. I would sign off on these payments under my code name, Oracle. At the meetings in the hotel, other agents were sometimes present.

15. My handlers also gave me an email address under an alias to use to send time-sensitive information that could not wait until our next meeting, such as a Muslim's imminent travel plans.

16. Agents Allen and Armstrong monitored and supervised my work as an undercover informant quite closely. Through my notes and our twice weekly meetings, I told them everything I was doing and every piece of information I could recall. They gave me instructions, or "tasking orders," regularly. They gave me both standing instructions on kinds of information to gather whenever I could—for example, to meet and get contact information for a certain number of Muslims per day—and also gave me specific instructions either in response to information I provided or based on information they wanted—such as, for example, instructions to get inside a certain house within the week or to have lunch with a particular person two times. My handlers also gave me standing orders to call one of them every day, even on my days off. I did this, and I would call one or both of them each day to apprise them of my day's activities.

17. Agents Allen and Armstrong did not, however, limit me to specific targets on which they wanted information. When I first met with Sadullah Khan at ICOI and began infiltrating the community, my handlers did

not give me any specific targets, but instead told me to gather as much information on as many people in the Muslim community as possible. For example, my handlers at first told me I would make my initial contact with the community by attending services at a mosque in Anaheim, but eventually advised me to attend ICOI instead because it was closer to where I lived, so I could spend more time there.

18. My handlers told me to look for and identify to them people with certain backgrounds or traits, such as anyone who studied *fiqh*, who openly criticized U.S. foreign policy, including the U.S. military's presence in Muslim countries; who had any kind of military training; who was an imam or sheikh; who went on *Hajj*; who played a leadership role at a mosque or in the Muslim community; who expressed sympathies to *mujahideen*; who was a quiet loner; who was a "white" Muslim; or who went to a *madrassa* overseas. But my handlers did not tell me to limit the information I collected to those people. They would occasionally take people I identified and tell me to spend more time with them or find out more about them, but these were always people I identified to them during the course of the operation, not people who had been targeted from the outset. I had no specific targets at the outset. To the contrary, my handlers tasked me with immersing myself in the Muslim community and gathering as much information on as many people and institutions as possible.

My Assignments and Activities as an Undercover Informant

19. My handlers gave me a standing tasking order that applied throughout the duration of my undercover work to get as much information as possible on any Mus-

lim I came into contact with at the mosques or in the Muslim community. Agent Allen told me, "We want to get as many files on this community as possible." My handlers explained to me that the United States was five to ten years behind Europe in the extent of Islamic presence, and that they needed to build files on as many individuals as possible so that when things started to happen, they would know where to go. They said they were building files in areas with the biggest concentrations of Muslim Americans—New York; the Dearborn, Michigan area; and the Orange County/Los Angeles area.

20. One thing my handlers wanted me to collect was contact information, particularly email addresses and phone numbers. At times, my handlers even gave me a quota to collect contact information for ten new Muslims per day. I reported this information in my daily notes. My handlers also told me that they monitored my email and cell phones to obtain the telephone numbers and email addresses of people with whom I corresponded. Agent Allen instructed me to give out my cell phone number widely so that people would call me or give me their cell numbers in return, so that the FBI could collect those numbers. My handlers also instructed me to email frequently with people, so that the FBI could collect their email addresses. My handlers told me that they used the cell phone numbers and email addresses of individuals who contacted me to obtain information from those individuals' phone and email accounts, including the list of people they contacted. My handlers gave me a particular email address under an alias to which they instructed me to forward these emails.

21. Agents Allen and Armstrong told me that they kept the numbers and emails I collected in a database

that could be monitored for international calls, or cross-referenced against phone calls or emails to persons of interest who were believed to be linked to terrorism. They also told me that the emails could be used to determine if the person was visiting certain websites, and with whom they were emailing. I also joined email distribution lists for many of the mosques I surveilled so that I could obtain the mosque membership lists and all of the email addresses. I would forward messages from the mosques to the FBI so they would be informed about events and bulletins, and so they would have the email addresses of anybody else who received the message.

22. During the course of my work, I had discussions with my handlers about whether what I was doing was productive, and whether the information I collected was actually being used. They assured me that all the information I collected was retained, and that they didn't discard any of the information. My handlers also told me that this information was used to build files on individuals. My handlers told me that every person who I contacted—whose phone number I got, who I emailed, who I identified through photographs—had an individual file in which the information I gathered was retained.

23. My handlers also tasked me with gathering information on mosques in the Orange County and Los Angeles areas. They instructed me, among other things, to map the mosques by locating entrances, exits, rooms, bathrooms, locked doors, storage rooms, as well as security measures and whether any security guards were armed. In some mosques, I used hidden video equipment attached to a camera in my shirt button to take images of the layout of the mosque. My handlers informed me that this information would be used by the

FBI to enter the mosques in case they needed to raid it or if they needed to enter and place electronic surveillance equipment in them. My handlers also instructed me to try to get the security codes for the alarm systems at several mosques. I managed to obtain the codes for one mosque by arriving early for dawn prayer and watching the person who opened the mosque punch the code in. I gave this information to my handlers. My handlers told me that they had the security codes to at least one other mosque, as well. They told me that they used the security codes to send agents into these two mosques at night.

24. My handlers also tasked me with getting brochures on charities that were distributed in the mosques, visiting the mosques' libraries or book areas to look for extremist books, collecting newsletters and bulletins to see what activities were going on in the mosque, and collecting names of individuals who attended, as well as their cell phone numbers and license plates.

25. In addition to information about the membership of each mosque, my handlers also wanted the names of all board members, imams, people who taught classes at the mosques, and other leadership within the mosques.

26. Over the course of my work, I went to about ten mosques and conducted surveillance and audio recording in each one. I spent the most time at ICOI, which I attended daily, but I spent significant time at other mosques, including the Orange County Islamic Foundation mosque in Mission Viejo, Durul Falah in Tustin, Omar al-Farouq mosque in Anaheim, Islamic Society of Orange County in Garden Grove, Al-Fatiha in the West Covina/Azusa area, the mosque in Lomita, and King Fahd mosque in Culver City. For about five or six

months I went at least once a week to each of these mosques. I would go to as many as four different mosques in a day. Even if I didn't pray at each mosque, I would go to the mosque and talk to people, or meet people at the mosque and go to the gym with them. I also went a few times to West Coast Islamic Center in Anaheim and a mosque in Upland.

27. Agent Armstrong told me that the FBI had every mosque—the ones I went to and the ones I didn't go to—under surveillance.

28. My handlers informed me that electronic surveillance equipment was installed in at least eight area mosques including ICOI, and the mosques in Tustin, Mission Viejo, Culver City, Lomita, West Covina, and Upland. He told me at one point that they could get in a lot of trouble if people found out what surveillance they had in the mosques, which I understood to mean that they did not have warrants.

29. At times, if I was left alone in a mosque office, I would look in drawers, which I understood to be consistent with my instructions to gather as much information as possible. I wrote these incidents up in my supplemental reports, and was never told not to do this.

30. My handlers instructed me to keep an eye out for people who tended to attract young Muslims and to identify and gather information on such people. They told me that they wanted to investigate anyone who had the attention of the youth or influence over young people to see if they were radicalizing them. For example, there was a popular youth group on Tuesdays at ICOI run by the imam, Sadullah Khan. Students from the Muslim Student Union at the University of California, Irvine ("UCI") would attend. To implement my han-

dlers' instructions, on many occasions I recorded the youth group meetings at ICOI by leaving my possessions, including my key fob, near where the group met in the prayer hall so that all of their discussions could be recorded. I did this by going into the prayer hall during their meetings to pray, and then leaving behind my possessions, as if I had forgotten them or just chosen to leave them there while I did other things. I would go to another part of the mosque or the courtyard, and return sometime later to collect my things. I told my handlers I did this in my written reports. My handlers never instructed me to stop this practice, and in fact discussed with me the contents of the recordings obtained in this manner.

31. Beginning in about September 2006, my handlers gave me a standing task to gather information on Muslims' charitable giving. My handlers instructed me to collect any pamphlet or brochure at any mosque that concerned charitable donations. They also told me to inquire of Muslims about which charities and *madrassas* to give to. I did this, and gave the names of the charities and *madrassas* to my handlers. My handlers specifically told me to ask people about *madrassas* or charities sympathetic to the *mujahideen* or *jihad*; to inquire about charities providing money to Somalia, Yemen, Pakistan and Afghanistan; and to inquire about money going to Lebanon and Palestine. They also instructed me to ask people how to avoid having my donations traced by the U.S. government. My handlers said that if a worshipper paid by check, the FBI could trace that check from the person's bank account to the organization. My handlers, in several conversations, told me that the FBI would open a file on any person who wrote a check to

any Islamic charity they were interested in, not just those officially designated as terrorist organizations.

32. My handlers also instructed me to attend Muslim fundraising events, to interact with the community and gather information, to identify people who attended and who they came with, and, if there were any speakers, to record what those speakers said. On my handlers' instruction, I attended a benefit for ICOI at a hotel in Irvine, where on their orders I purchased a vase for about $900 to bolster my credibility among the community.

33. My handlers also instructed me to attend lectures by Muslim scholars and other guest speakers. I attended lectures of Yusuf Estes, a white Muslim scholar from Texas, and Hamza Yusuf, another white Muslim scholar from Oakland. My handlers wanted to know both what the lecturers said and who attended these lectures, so they set me up with a video surveillance device that had a camera in a shirt button. I went early and got a seat in the front row where I could clearly record the lecture. Afterwards, when people were socializing, I walked around filming attendees with my camera. I also collected license plate numbers from the parking lots to identify those who attended.

34. During my time working on Operation Flex, I told people in the Muslim community that I worked as a fitness consultant. In about November 2006, Agent Allen instructed me to start going to the gym to work out with people I met from the Muslim community in order to get close to them and obtain information about them. They did not limit the scope of their instructions; the directive included anyone from any mosque without any specific target, for the purpose of collecting as much in-

formation as possible about Muslim men in the community. I went to various 24-Hour Fitness and L.A. Fitness gyms around the Orange County area. These workouts provided an easy opportunity to talk with people and to elicit a wide variety of information pursuant to my handlers' instructions. For example, I would talk to people about their lives and get information about their problems that my handlers could use to pressure them to provide information or become informants. I also learned people's travel plans and their political or religious views, and could elicit responses that the FBI might use to justify further surveillance by asking pointed questions about Islam or politics. I recorded these conversations using the equipment on my key fob or cell phone. This surveillance was so fruitful that my handlers eventually told me they were seeking approval to have me open a Muslim gym.

35. During my regular meetings with my handlers, they showed me photographs of Muslims from the community and asked me to identify the people in them. Frequently, these were photographs of people I worked out with taken at the entrance to the gym. My handlers told me that they had an arrangement with the gyms to obtain photographs from the security cameras. Other photographs came from parking lots, parks, restaurants, or other public places. When I asked how they got the other photographs, they told me they had "assets in place." They asked me to provide as much information as possible about each person—they told me to "empty my head" on the individuals. They wanted to know, among other things, what mosque they attended, their ethnicity or country of origin, the languages they spoke, the people they associated with, what kind of car

they drove, their occupation or whether they were a student, as well as any other information I could obtain.

36. Agent Allen told me that Islamic restaurants in Anaheim and Irvine were under video surveillance, so they could see who associated with whom. Agent Allen also said they surveilled soccer and basketball games for the same reason. I frequently met people in restaurants and cafés and recorded conversations there.

37. I also had standing orders to enter and observe Muslim schools whenever possible. When I first reported entering a Muslim school, my handlers questioned me intently on whether I had witnessed children chanting from the Quran. When I said I hadn't, they asked me again and told me that if I had, that would take the case to a "new level." My handlers more than once told me to look for Quranic reciters at the schools. My handlers also instructed me to look for photos of extremists, books by extremists, and whether the children were learning subjects besides Islam, like math, English or history. My handlers said that they did not want an Islamic school to be an "American *madrassa*."

38. I attended an Arabic language class at ICOI from about December 2006 to March 2007. My handlers instructed me to obtain the lists of the individuals who attended the class, which I provided to my handlers. My handlers told me that they retained the information about who took the class.

39. I also attended a course in *fiqh*, or Islamic law which pertains to morals and etiquette. My handlers were interested in *fiqh* because parts of *fiqh* address military training. At my handlers' request, I got a copy of the list of people who attended the class. Because this list included the languages that class members spoke, it

provided a clear indication of their ethnicity or country of origin as well.

40. My handlers were only interested in Muslims, and set aside any non-Muslims who were identified through surveillance I performed. For example, on several occasions when my handlers asked me to identify individuals from photographs taken by surveillance cameras at the entrances to the gyms, they would present me photographs of individuals who were not Muslim—usually Latino—whom I might have spoken to or who had simply helped me lift weights. When I indicated to my handlers that the individual was not a Muslim, the picture was discarded.

41. My handlers were interested in websites that they believed were jihadist, including *MissionIslam.com* and *CagePrisoners.com* (a site devoted to raising awareness about the detainees at Guantanamo Bay). Agent Allen told me to encourage people I spoke with to go to these websites because they could document people's visits to the website and use that either to pressure them to become informants or to justify further surveillance on them.

42. My handlers encouraged me to bring up Muslim scholars and thinkers who they believed were extremist in my conversations with individuals in the community. This included Hassan al-Banna, Sayyid Qutb, Sheikh Suhaib Webb, Yusuf al-Qaradawi, Yusef Estes, Ayman al-Zawahiri, Anwar al-Awlaki, and others.

Increasing Infiltration of the Muslim Community

43. The people I met at the mosques helped me learn how to pray, learn how to dress, and learn Islamic culture and etiquette. My handlers told me to allow Mus-

lims I met to "radicalize" me gradually, and saw the help the community was giving me as the first steps toward such radicalization. I felt the people who helped me were sincere in wanting me to develop in my Muslim faith and wanting to have me as part of the community and part of the mosque. My handlers instructed me not to talk too openly about *jihad* at first, but to go to prayers at the mosque and be seen. My handlers were very pleased that I developed a rapport with the community so quickly.

44. As months went on and I was increasingly accepted by the Muslim community and the leadership at mosques, and I continued to work generally six or seven days a week, my handlers seemed to place increasing trust in me. While at first they told me as little as possible about what else they knew about the community and what other intelligence efforts were ongoing, after several months they began to tell me more about what other kinds of surveillance they were undertaking, how they knew certain things, and how the intelligence I gathered was being used, so that I could understand how to work effectively.

45. In about October 2006, on the instruction of Agent Allen, I began to try to appear more Muslim. I went to the mosque early and prayed loudly, and wore traditional clothes that people at the mosque had given me. My handlers told me that nobody in the community leadership, people of interest, or youth suspected that I was an informant. I asked how he knew, and he eventually told me that they listened to a number of conversations in which people were discussing me outside. I realized that these were conversations that I could not

have recorded, which meant that my handlers were getting this information from other electronic surveillance.

46. My handlers also instructed me to start attending *fajr* (dawn) prayers, which are held about 4 a.m., or *ishaa* (late) prayers, which are held about 9:30 p.m. My handlers told me that people who attended prayers very early in the morning or late at night, and especially both, were very devout and therefore more suspicious. They instructed me to obtain the names and the license plate numbers of individuals who attended these prayers. When I agreed to go to *fajr* prayer four days a week, my pay increased substantially.

47. My handlers instructed me to memorize certain *ayas* and *surahs* (verses and chapters from the Quran) and to ask Muslims about them. My handlers told me that they had picked these verses because they believed them to be susceptible to a jihadist interpretation, so that people's reactions to them would help discern who was and was not a threat. They told me that discussions about these verses would elicit responses that could be used to justify additional surveillance measures. A true and correct copy of a tasking order in Agent Allen's handwriting specifying certain verses is attached hereto as Exhibit A.

48. My handlers also instructed me to elicit reactions from people by talking provocatively about U.S. foreign policy—for example, by raising the issue of civilian Muslim men, women, and children killed in conflicts in Iraq, Afghanistan, Palestine, and Lebanon. By stirring people to speak out of anger, they told me, I could again elicit responses that could be used to justify additional surveillance measures against those people.

49. Beginning in about January 2007, an individual who called himself George began coming roughly every month to meetings with my handlers. George said he was "from Langley," which I understood to mean that he worked for the Central Intelligence Agency headquartered in Langley, Virginia. When I once mentioned him as working for the CIA, Agent Allen said something to the effect, "We don't say that. Say he is 'from Langley.'" No one ever told me George's last name. George spoke Arabic very well and knew a great deal about Islam—he would speak Arabic with me and comment on my improved fluency, as well as ask me questions about Islam and the Quran to monitor my progress in acquiring the appearance of being a devout Muslim. George also instructed me on my grooming and physical appearance to make it seem that I was increasingly devout. For example, at one point he instructed me to develop a sore on my forehead from bending my head to the carpet in prayer, to make clear that I was praying all the time.

50. On about four different occasions, during the meetings with my handlers at the hotel room, they showed me a huge photo array on a large board consisting of the photos of around two hundred Muslims from the Orange County/Los Angeles area. My handlers used different sets of photographs for each of these meetings, so showed me many hundreds of photographs over the four meetings. They instructed me to arrange the photos from the most dangerous to the least based on my knowledge and experience. The entire leadership of the Islamic community were in the photos—sheikhs, imams, board members, prayer leaders, leaders of civic organizations, and youth groups. It took hours. They also asked me to assist them in organizing the photos according to categories such as financial, operative, and lead-

ership. We also divided photos into possible cells according to mosques and ethnicity or nationality. I did not know all of the people in the photographs, but my handlers had information on people I did not know enough to place them in the various arrangements. The first of these meetings was in about March 2007, and the last was in about September 2007.

51. Over the course of several conversations, my handlers told me that they considered the leaders in the Muslim community—board members and leadership at mosques and leaders of Muslim organizations—to be potential threats and that they regularly surveilled them and maintained more detailed files of information on their background and activities. They told me that the leadership of the community could give orders or *fatwas* that someone in the community would carry out.

52. Because I was single in my undercover identity, people in the community considered me an eligible Muslim and various individuals wanted to introduce me to Muslim women. Agents Allen and Armstrong, and George from Langley, wanted me to date as a way to get information. When I asked how I should go about dating, and what happened if things began to get intimate, my handlers told me that if I was getting good information, I should let things "take their natural course," and then they said "just have sex." I had sexual relationships with women in the Muslim community for the purposes of information gathering pursuant to these instructions.

53. My handlers were always interested in obtaining new informants within the Muslim community. They spoke to me about "MICE," an acronym for Money Ideology Compromise Ego, or the various ways people can

be convinced to be informants. They often focused on the element "compromise," which consisted of obtaining information on potential informants that could be used against them if they refused to inform. Subjects that would potentially lead to compromise included immigration issues, sexual activity, business problems, or crimes like drug use. My handlers instructed me to pay attention to people's problems, to talk about and record them. I reported problems that several individuals told me about, including marital problems, business problems, and petty criminal issues. My handlers on several occasions talked to me about different individuals that they believed might be susceptible to rumors about their sexual orientation, so that they could be persuaded to become informants through the threat of such rumors being started, even though my handlers had no evidence that such rumors would be true.

54. My handlers also often referred to the principle that "everybody knows somebody." They explained that if someone is from Afghanistan, that meant that they would likely have some distant member of their family or acquaintance who has some connection with the Taliban. If they are from Lebanon, it might be Hezbollah; if they are from Palestine, it would be Hamas. By finding out what connections they might have to these terrorist groups, no matter how distant, they could threaten the individuals and pressure them to provide information, or could justify additional surveillance.

55. On one occasion, my handlers instructed me to develop my relationship with a person who told me that his father was sick in a foreign country and in a lot of pain. I had a significant amount of Vicodin, a prescription pain reliever, left over from a surgery I had previ-

ously undergone. I discussed with Agent Allen that providing this person some Vicodin would help build the relationship and build my reputation as a devout Muslim who had access to black market items. Agent Allen instructed me to provide the person with 60 tablets of my leftover Vicodin, which I did. On another occasion, Agent Allen instructed me to provide prescription anabolic steroids to another two individuals to similarly further my credibility, which I did.

56. In about early spring of 2007, after I provided some information my handlers believed was very valuable, my handlers told me, "You're gold in L.A. You're gold in Washington." They said that higher ranking officials wanted to use me in other places as well. Agent Allen told me several times that information I provided had been used in presidential daily briefings. They told me that my work was followed by people "at the highest levels." They told me that the operation I was working on was among the ten most important intelligence investigations going on in the country. Agent Allen told me in about March or April 2007 that he had meetings with Stephen Tidwell and one of his supervisors from Washington, D.C., Joseph Billy, Jr., about the operation. Around the same time period, Agent Allen told me that he had to fly to D.C. with his supervisor, Pat Rose, in part to meet with high-level FBI officials to get approval to open a gym for Muslims that would function in part as a mosque with a prayer room, and that I would run. He called me from D.C. to tell me that the gym had been approved.

57. During about spring 2007, Agent Allen told me that I needed to be careful how I wrote my notes, and that I needed to be very precise and detailed, because

people in Washington were reading and summarizing the reports to make things "sexier" than I had intended so as to accomplish their own goals. He told me that I needed to be careful always to use precise and detailed language so that more could not be read into the reports than I intended.

58. During the course of the operation, I learned there were a large number of FBI informants in the Orange County Muslim community. My handlers told me at various times that the Muslim community was "saturated" or "infested" with informants, and said it was like the societies of cold war East Germany and Cuba, where everyone was informing on one another. During the meetings in the hotel room when my handlers and I arranged photographs of people in the Muslim community, many of the photographs had asterisks by the names. Several of the people marked were people my handlers had already told me were informants, so I asked my handlers if the asterisks indicated informants, and they eventually confirmed that they did. At each of the four meetings, there were dozens of people labeled as informants, and I believe over the four meetings I saw well over one hundred people marked as informants. I personally interacted with more than forty people my handlers told me were informants. My handlers told me that the other informants had been recruited from the community because the FBI had pressured them in some fashion, and they told me that they did not trust the informants they had recruited from within the Muslim community.

59. As I continued as a constant presence at ICOI and the community became more comfortable with me, I began to participate in the prayers to a greater degree.

I gave the *adhan*, or call to prayer as well as the *al-Fatiha*, or opening to the evening prayer. On a few occasions, when prayer leaders went out of town, I led the *dhuhr*, or midday prayers, and the *fajr*, or dawn prayers. My handlers were extraordinarily happy that I had been given the responsibility to lead prayers, as they believed it showed an acceptance of me by the community.

60. After several months of working, my handlers told me more about how some aspects of their investigation worked. Agent Armstrong told me that although the terrorist watchlist was maintained by the Department of Homeland Security, the information in that list was based on information collected by the FBI. He told me that information I collected would get shared with Homeland Security and other agencies. For example, my handlers were interested in travel plans of Muslims—after a while I asked why they wanted to know. They eventually indicated that the reason they wanted to know this was to share it with Homeland Security to monitor or search people during their travels.

61. My handlers also told me that information I obtained would be shared with other agencies. They told me that information I obtained on finances or foreign assets was shared with the Treasury Department. Several times when I had information about people's immigration issues, my handlers told me that they would send the information to immigration officials. My handlers told me that they were "in the business of sharing information" about terrorism with other agencies.

62. I also learned about the voluntary interviews the FBI would ask of people from the Muslim community. My handlers told me that they would usually bring people in to an FBI interview only after I had obtained some

useful background on the person—usually by recording some embarrassing personal information or a statement of political beliefs that they would not want to admit to the FBI. They could then use that information to pressure the person to provide information, or could ask about that information in order to get the person to deny it, which would set up the allegation that they had lied to the FBI during the interview, which would in turn provide leverage to get the person to provide information. They told me that they tried to put interviewees at ease by saying that they were investigating someone else.

63. It became clear to me that there was audio surveillance either on the telephones or in offices of a large number of leaders in the Muslim community. For example, on one occasion around when ICOI was attempting to get a restraining order against me, some people were saying I was an informant. At that time, Agent Allen called me and said words to the effect, "You need to call [Person A] right now. He's on the fence about you and talking to [Person B] on the phone right now. Call him and break in and take him to dinner." I could hear the voices of the people he was talking about in the background. Agent Allen made similar calls to me several times about different people.

64. During many conversations with my handlers over the course of my work, my handlers told me that not everything our operation was doing was legal. My handlers told me that because the U.S. was fighting an enemy that was not sovereign, they had to carry out policies that were contrary to the Constitution.

65. On several occasions in restaurants, I left my recording devices (a key fob or my cell phone) in a place

where it could record a conversation while I went elsewhere. Sometimes I did this with groups that met in the mosques: if there was a youth group or a group that met with a particular scholar, I went over to put down my things, including the recording device, and greet people, then went to a different part of the room to pray. In restaurants or cafés, too, on more than one occasion when I was speaking to one group and saw another group come in, I moved to the new group while leaving my cell phone at the first so as to record both conversations at once. I stated that I did this in my notes to my handlers and was never instructed to stop.

66. On several occasions, I left my recording devices in locations in mosques in the area. For example, in King Fahd Mosque in Culver City, several times I came in with a friend who changed in the office from business clothes to more traditional dress before we went into the mosque to pray. While he did so I left my keys in the office so that the key fob would record staff and board members who came in and talked. I retrieved my keys from the office when we were finished in the mosque. I did this several times, and in several different mosques. I stated that I did this in my notes to my handlers and was never instructed to stop.

67. I once asked Kevin Armstrong about covert video recording surveillance he had told me was being conducted at a local bookstore. He said that while you needed warrants for criminal investigations, "National security is different. Kevin is God." I understood him to mean that he did not have warrants for the surveillance at the bookstore. Agent Armstrong also told me on more than one occasion that they did not always need warrants, that if they did not have a warrant they could

not use the information in court, but that it was still useful to have the information. He mentioned that they could attribute the information to a confidential source if they needed to.

68. In about June 2007, my handlers told me the FBI was planning an action to make a number of arrests based on intelligence that I had gathered. My handlers took me to the Anaheim Hilton hotel where I stayed out of contact for several days at the FBI's expense. My handlers told me that the operation would soon be over. My handlers told me that more than seventy agents had amassed in the Santa Ana office to conduct pre-dawn arrests of twenty-seven people, but that the office of FBI Director Mueller had called from Washington, D.C., and ordered the agents to stand down and not go through with the arrests. My handlers were very upset about this. After the aborted arrests, I returned to my role as an undercover informant, doing exactly the same work as before.

69. Both my handlers and other agents explicitly told me that Islam was a threat to America's national security.

70. One individual I made contact with had a pending federal criminal case. Agent Armstrong, who was a former Assistant U.S. Attorney, initially told me to be careful not to discuss his case because there would be problems because he was represented by counsel. But he was overruled by others, including Agent Allen, and I was then instructed to talk with him about his case. I understand that the information I gleaned was used in his criminal case.

71. Over the course of fourteen months of working as an informant in the Los Angeles and Orange County

Muslim community, I estimate that, on my handlers' instructions, I passed hundreds of phone numbers and thousands of email addresses of Muslims to the FBI. I provided background information on hundreds of individuals. I made hundreds of hours of video recordings that captured the interiors of mosques, homes, businesses, and the associations of hundreds of people. I made thousands of hours of audio recording of conversations I participated in and where I was not present, as well as recordings of public discussion groups, classes, and lectures.

Termination of My Assignment

72. In about March 2007, Agent Allen provided me a written letter from an Assistant U.S. Attorney named Deirdre Eliot to engage in jihadist rhetoric and to engage in other criminal activity with immunity. I understand that this letter gave me blanket immunity for all my conduct as an undercover informant. I signed the letter, but Agent Allen took the letter back and did not allow me to keep a copy.

73. My handlers had instructed me to ask general questions about *jihad* from the beginning of my assignment. In early 2007, my handlers instructed me to start asking more pointedly about *jihad* and armed conflict, then to more openly suggest my own willingness to engage in violence. In one-on-one conversations, I began asking people about violent *jihad*, expressing frustration over the oppression of Muslims around the world, pressing them for their views and suggesting that I might be willing or able to take action. In about late spring of 2007, people at ICOI began to get concerned about me. After one incident where I said some extreme things in order to test the reaction of others, several in-

dividuals reported me to local police and to the FBI. When the authorities did not respond with any urgency, people became suspicious that I might be working for the FBI. Congregants at ICOI brought an action for a restraining order to bar me from the mosque. On June 19, 2007, I understand that there was a hearing in which testimony was presented and the restraining order issued barring me from entering the mosque. I continued my undercover work at other mosques in the area, but the restraining order and the fact that various members of the community had become suspicious about me made it much more difficult to get close to people and to gather information.

74. During the time ICOI was attempting to obtain a restraining order against me, Agent Allen instructed me to go back into the mosque. I feared for my safety since I knew some people suspected I was an informant. I told Agent Allen I would only go in if I was armed with a knife, and that I would defend myself if someone gave me reason to. My handlers acknowledged what I said, but did nothing to stop me from doing so. I went into ICOI on two subsequent occasions with a knife strapped to my leg.

75. At some point during the spring of 2007, my handlers mentioned to me that the Assistant Director in Charge of the FBI's Los Angeles Field Office had told the Muslim community that there would be no undercover informants placed in mosques at a meeting held only about a month or so before I had taken *shahaddah*. The Assistant Director in Charge at that time was Stephen Tidwell. I was surprised, and my handlers said that, at that time, they had already been looking for

someone to send into the mosques and Tidwell had approved recruitment of an informant.

76. During the summer of 2007, around the time ICOI was seeking the restraining order and afterwards, I was repeatedly approached for an interview by a reporter from the Los Angeles Times named H.G. Reza. My handlers disliked this reporter—they told me that he was an enemy of the United States and that he was under surveillance. On one occasion, my handler called me to tell me not to go to a particular gym because Reza was waiting for me in the parking lot. When I asked him how he knew that, he said "We're the fucking FBI. We know everything." In October 2007, FBI counsel Stephen Kramer paid me $25,000 cash to assure that I would not disrupt the rest of the case, and explicitly told me that the payment was in part so I would not speak with Reza.

77. In about June 2007, when some people in the community were beginning to suspect I was an informant, I had discussions with my handlers about being paid substantial additional sums of money to go to jail or prison to help bolster my credibility in the community and convince people that I was not a confidential informant. We discussed having me very publicly arrested in the parking lot of a mosque, and the details of the pay and arrangements to make life tolerable in prison. My handlers eventually told me that this plan failed because a federal judge had refused to go along with it.

78. During about the summer of 2007, my handlers told me that the Assistant Special Agent in Charge in Santa Ana, Barbara Walls, did not trust me and did not want me working any more. They told me there was significant conflict between Agent Walls and field agents

over how to handle the operation, and that there had been an audit team sent from Washington, D.C., to examine Agent Walls' handling of one potentially valuable piece of information I provided. Because of this conflict and complications surrounding the restraining order, my handlers told me in about September 2007 that I would be going on "hiatus" from my undercover work in the Orange County Muslim community.

79. During one of my final meetings with my handlers, at which Agent Walls was also present, she warned me to stay silent about my participation in the operation. She said that if word got out that the FBI had sent an informant into mosques and the community, that it would destroy the relationship between the Islamic community and the FBI. She said that "we assured them" that the FBI would not send undercover informants into mosques.

80. In October 2007, I had a last meeting, where my handlers had instructed me to bring back the laptop computer and surveillance equipment they had issued me. I said to them that I guessed the operation was over. Agent Allen said emphatically no, the operation had just begun. He said that my role was over, but that Operation Flex and the FBI's operations in Orange County and Los Angeles would continue. He also said that the information I had provided was an invaluable foundation for the FBI's continuing work. He also said that after some down time, I would have the option of working in New York or other places.

81. Prior to February 2009, I never confirmed to anyone outside of law enforcement and my immediate family that I was working as an informant for the FBI. That month, FBI Agent Thomas Ropel III testified in a bail

hearing in a federal criminal case about information used in that prosecution that he said had been provided by an undercover informant, and described the undercover informant such that many people in the Muslim community could clearly identify the informant as me. Several days later, an article appeared in the Los Angeles Times containing statements I made to a reporter about being an FBI informant. I am not aware of any information either publicly released by the FBI or otherwise available to any member of the Orange County Muslim community prior to February 2009 that would allow them to do anything more than speculate that I might have been an FBI informant.

Ongoing Surveillance

82. Between about December 2007 and August 2008, I was incarcerated for reasons that are currently the subject of a federal civil action against the Irvine Police Department, the FBI, and others. Concerning that matter, my handlers told me that their supervisors in the FBI office did not want me to be publicly identified as an FBI informant, so I ended up pleading guilty on their instructions, and spent eight months in jail as a result.

83. After I got out of prison in about August 2008, I contacted the Irvine Police Department to voice concerns about my safety from members of the Muslim community that might suspect me of being an informant. I was visited by a detective, as well as a sergeant that I recognized as someone who had once escorted me when I was undercover with my handlers. The sergeant knew very specific information about individuals I had surveilled who I had concerns about, and told me in this meeting that he worked for JTTF. He told me that several individuals I asked him about were still under sur-

veillance. He also specifically mentioned that surveillance was ongoing at gyms and at least two mosques.

84. In recent months, I have begun returning to local gyms where Muslims work out. In one gym in Irvine, on two different occasions since about September 2009, I saw a Muslim who I knew to be an informant, who looked at me and quickly looked away guiltily. Both times I saw the informant, when I went out to the parking lot, I saw a white SUV with people inside who I recognized as members of the JTTF that I saw when I worked undercover. On one of these occasions, I saw one of the individuals holding a camera in both hands as if he were using it. They saw me, looked surprised, and also looked away. I believe that they were actively engaged in surveillance of the gym, perhaps through the informant.

I declare under penalty of perjury of the laws of the State of California and the United States that the foregoing is true and correct. Executed this 23rd day of April, 2010 in Orange, California.

/s/ CRAIG F. MONTEILH
CRAIG F. MONTEILH

DECLARATION OF CRAIG F. MONTEILH

I, Craig F. Monteilh, make this declaration of my own personal knowledge and if called to testify, I could and would do so as follows:

1. From about July 2006 until about October 2007, I worked for the United States Federal Bureau of Investigation ("FBI") as an undercover informant assigned to infiltrate the Muslim community in Southern California. During this time, I generally spent about six or seven days a week posing as a Muslim convert named Farouk al-Aziz, conducting surveillance and gathering information on a wide variety of individuals and organizations in the Muslim community. My "handlers," or the FBI agents who directed my operations, during this time were FBI Special Agent Paul Allen and FBI Special Agent Kevin Armstrong.

2. On my handlers' instructions, I made audio recordings of everything I did while working as an informant, including all the conversations I had, using recording devices they had given me. I recorded all day, every day. My handlers told me that if something was not recorded, it was as if it didn't happen.

3. My handlers were interested in the mosque at Mission Viejo, the Orange County Islamic Foundation ("OCIF"). They considererd the imam of the mosque, Yassir Fazaga, to be a radical for several reasons: My handlers told me Fazaga directed students on how to conduct demonstrations and encouraged them to speak out. They told me that when the FBI Assistant Director in Charge of the Los Angeles Field Office, Stephen Tidwell, attended a meeting at an Orange County mosque in about spring 2006, Fazaga openly pressed Tidwell about FBI informants in mosques, and when Tidwell de-

nied putting informants in mosques, Fazaga had openly said he did not believe Tidwell. My handlers also told me Fazaga was a person of interest because he was a board member of "In Focus News," a prominent Muslim newspaper that was vocal in speaking out against U.S. government actions that negatively affected Muslims and which my handlers believed was anti-American and linked to Muslim civil rights groups.

4. My handlers also believed that OCIF was linked to another mosque they were interested in, the Islamic Center of Irvine, because the two mosques held joint events and jointly organized foreign trips, including the *hajj* pilgrimage to Mecca. They referred to OCIF as a "definite hotspot."

5. My handlers also believed that the mosque was radical because it had certain religious scholars as guest speakers who my handlers believed were radical—particularly Yusef Estes, Suhaib Webb, and a local imam, Ahmad Sakr. My handlers told me that a moderate mosque would not have chosen these guest speakers. On my handlers' instructions, I attended the Yusef Estes lecture and video recorded the event using a camera hidden in a shirt button that my handlers provided. On my handlers' instructions, I video recorded the entire lecture, the literature Estes had set out, and the people who attended.

6. I attended OCIF a number of times to conduct surveillance.

7. On my handlers' instructions, I used a video camera hidden in a shirt button that my handlers provided me to take video of the interior of OCIF. My handlers instructed me to get a sense of the schematics of the place—entrances, exits, rooms, bathrooms, locked

doors, storage rooms, as well as security measures and whether any security guards were armed. I understood that this information would be used to place surveillance equipment inside the mosque. I later asked Agent Armstrong if they had used the information I had gathered to enter the mosque, and he said that they had.

8. On my handlers' instructions, I also made video recordings of an area in the back of the mosque where there were religious books available for congregants to use, so that my handlers could determine if any of the literature there was extremist.

9. My handlers instructed me to make contacts within the Mission Viejo congregation. I worked out on various different occasions with about 40 of their congregants, usually in groups. For anyone I worked out with, I got their email address and cell phone number and passed that information on to my handlers. I understood from my handlers that the FBI used this contact information to further track these individuals' communications and conduct surveillance of them.

10. My handlers instructed me to gather additional information on a few individuals within the congregation who seemed to have the most direct access to Fazaga. I talked to these individuals and obtained their email addresses, cell phone numbers, and addresses, as well as basic background information such as their occupation, whether they were married or had children, and what prayers they attended. I passed the information on to my handlers.

11. My handlers instructed me to monitor Fazaga at the prayers he conducted: to record and report on what he said, to talk with him afterwards and see who else talked to him afterwards, and to note individuals who

appeared to be close to him. They wanted me to get into a circle of people close enough to Fazaga that he would talk freely in front of me. I also monitored what was said by a member of the congregation who substituted for Fazaga during one of the prayers I attended.

12. It was significant to my handlers when a prominent member of the community introduced me to Fazaga while I was recording with a hidden video camera, in about April 2007. At that meeting, I asked Fazaga to work out with me and he agreed. My handlers were excited by this prospect, but I never actually worked out with him. I obtained Fazaga's cell phone number and email address (not through Fazaga, but through others) and passed these on to my handlers. My handlers told me they used the email addresses and telephone numbers I gathered to monitor communications and conduct further surveillance.

13. I also passed to my handlers the license plate numbers of cars Fazaga traveled in and the people I saw him associate with.

14. My handlers told me that there was another informant within the mosque with access to Fazaga, but that they did not fully trust him, so I was tasked with getting close to him to establish his reliability. My handlers also told me there were a number of other informants at the mosque, but that they did not have access to the imam.

15. My handlers instructed me that whenever I saw Fazaga at another mosque or anywhere outside OCIF, I should call them and let them know immediately. I did this at least once when I saw him at another mosque.

16. On one occasion, during Friday afternoon prayer at OCIF, the mosque had booth set up to collect donations for a cause—I believe for some kind of relief for Muslims abroad. Pursuant to my handlers' standing orders that I monitor donations, I stood near the booth and used the hidden video camera I was wearing to make video recordings of people who went up to the booth to contribute money.

17. I never observed anything that gave me any reason to believe that Fazaga or any of the congregants or leadership of OCIF were involved in violence or terrorism in any way.

I declare under penalty of perjury of the laws of the State of California and the United States that the foregoing is true and correct. Executed this [11]th day of October, 2010 in Los Angeles, California.

/s/ CRAIG F. MONTEILH
CRAIG F. MONTEILH

DECLARATION OF CRAIG F. MONTEILH

I, Craig F. Monteilh, make this declaration of my own personal knowledge and if called to testify, I could and would do so as follows:

1. From about July 2006 until about October 2007, I worked for the United States Federal Bureau of Investigation ("FBI") as an undercover informant assigned to infiltrate the Muslim community in Southern California. During this time, I generally spent about six or seven days a week posing as a Muslim convert named Farouk al-Aziz, conducting surveillance and gathering information on a wide variety of individuals and organizations in the Muslim community. My "handlers," or the FBI agents who directed my operations, during this time were FBI Special Agent Paul Allen and FBI Special Agent Kevin Armstrong.

2. On my handlers' instructions, I made audio recordings of everything I did while working as an informant, including all the conversations I had, using recording devices they had given me. I recorded all day, every day. My handlers told me that if something was not recorded, it was as if it didn't happen.

3. In some of my earliest meetings with my handlers, they showed me a picture of a young man named Ali Malik. They told me he had been a surfer kid in Newport Beach who wore dyed hair, but had travelled to Yemen to attend a madrassa, and had returned to the U.S. wearing traditional Muslim dress and a full beard.

4. My handlers told me Malik's change in behavior in embracing religion and traditional dress was highly suspicious and for that reason they needed to investigate him. They also told me they were suspicious of Ma-

lik because he was involved with people from the "MSU." "MSLJ" stands for "Muslim Student Union," which is the name of Muslim student groups at many colleges and universities, including U.C. Irvine. My handlers told me that they were investigating several individuals who were part of the MSLJ at U.C. Irvine, because they thought these individuals had ties to extremists, they thought that an imam who helped found the MSUs was radical, and they did not like the MSU's activities because it organized demonstrations and was vocal in its criticisms of IJ.S. foreign policy. They mentioned several times a mock wall at U.C. Irvine that the MSU had created that was supposed to represent the wall between Palestine and Israel. They said that the MSU was under surveillance and had its own separate task force dedicated to that surveillance. But they also used the term "MSIJ" more broadly to include not just particular student groups on particular campuses, but young Muslims who were active in the Muslim religious community and who associated with other young Muslims who were MSU members. Malik was lumped in with the MSU because he associated with other people from the MSU at Irvine and other young Muslims, even though he did not go to U.C. Irvine.

5. My handlers also told me Malik's father was a hero who had fought against the Soviets in Afghanistan. This background was another reason they were suspicious of Malik.

6. Agent Armstrong told me that before he was assigned to be my handler, he had been assigned to investigate the MSUs and young Muslims, including Ali Malik.

7. My handlers told me that the way that Malik groomed his beard indicated that he was a radical.

8. My handlers already had a significant amount of information on Malik and his family before I was assigned to do anything. They wanted me to get more information on one of his brothers; on another individual who Malik was close to; on Malik's associations from the Irvine mosque, and on who Malik hung out with at the gym.

9. My handlers said that they knew Malik had been to a madrassa (an Islamic religious school) in Yemen, but did not know the name of the school. They also told me that they knew he had been blocked from entering Saudi Arabia after he had traveled to Yemen, but they did not know why. They tasked me with finding out what school he had been to and why he had been denied entry into Saudi Arabia.

10. Very soon after I formally converted to Islam, I met Malik at the gym and began talking to him. I also spoke with him at the mosque. Sheikh Sadullah Khan saw me talking to him at the mosque and asked Malik to show me how to pray. Malik willingly helped me. He also bought me a very basic book on Islam. On the instructions of my handlers, I later used this book to ask Malik about the sections of the book that mentioned jihad, in hopes of eliciting some response that might incriminate Malik or justify further surveillance. I recall that Malik told me that the best interpretation of jihad was as "spiritual" jihad, or the personal struggle to improve one's life. On my handlers instructions, I also asked him about certain imams and religious scholars in order to discern his religious views, and pressed him on questions of U.S. foreign policy, in an attempt to record

him saying something that could be construed as extremist that would justify further surveillance, or possibly be used to pressure Malik to give information to the FBI. Malik seemed surprised by my questions during these conversations and repeatedly urged me to concentrate on learning the basics of Islam.

11. I saw Malik frequently during Ramadan in the fall of 2006, but after that only about once a week, at mosque or at the gym, and often in passing. My handlers urged me to have a meal or tea with Malik, and I tried to make plans several times, but he had a busy schedule and we never did. I would sometimes time my visits to a local gym to coincide with the time I knew he went there after his classes, and would try to talk to him at the gym, on my handlers' instructions.

12. Sometime in early 2001, Ali Malik suggested to me in some conversations that he was having problems with his wife, who lived in Chicago. When I reported this to my handlers, they told me that I should try to work out with Malik at the gym and act as a comforting friend in order to have him open up and offer information. On my handlers' instructions, I did this and recorded Malik talking about his marital problems. I provided these recordings to my handlers. My handlers told me the recordings would be useful in pressuring Malik to provide information, because they thought the recordings contained embarrassing facts he would not want revealed.

13. In about April 2007, my handlers started discussing the possibility of sending me abroad to a madrassa to study Islam and Arabic, in hopes that I would get sent from there to a terrorist training camp. I started asking about a school to go to, saying I wanted

to go to Pakistan. Malik told me that he had attended Dar al-Mustafa in Tarim, outside Sana, in Yemen. I reported this to my handlers, who were very excited about the information. Agent Allen moved quickly to investigate and told me it was a radical school and that he believed that Malik did not get into Saudi Arabia after his trip to Yemen because he had been studying at a radical school. My handlers also told me they thought people at the school could refer students to terrorist training camps, so that if I went, they might refer me to a camp.

14. I found out from the Dar al-Mustafa brochure online that I needed an imam's signature to apply. I approached Sadullah Khan, in about early May 2007, about going to the school in that summer. Khan said he would provide a letter for me, but I ended up not applying because people in the mosque got a restraining order against me.

15. My handlers thought Malik had ties to an organization, the "Islamic Society of North America" ("ISNA"), because it was headquartered in Chicago, where Malik's wife lived. My handlers instructed me to ask Malik about ISNA, which I did. Malik said they were doing good things, but did not indicate he was a part of it. I recorded these conversations and reported them to my handlers.

16. My handlers told me they thought Malik might be selling prescription drugs, because he did not have a job and had money to go out with friends, and to travel to see wife in Illinois. My handlers told me they thought this might be true of several young people at the Irvine mosque. I never discovered anything in any of my time undercover about Malik or any of the other young peo-

ple selling prescription drugs or engaging in other illegal activity to make money.

17. On several occasions, I used the recording devices provided to me by my handlers (disguised as a key fob or cell phone) to record groups of young Muslims talking in the prayer hall after *ishaa* prayer. On these occasions, I greeted people, left my things—including the recording device—near to where they were talking, then went to another part of the mosque or a different part of the prayer hall to pray so that my recording device would capture their conversation when they did not think I could hear. Several times Ali Malik was one of the people in the group I recorded. I recorded his conversations when I was not present, then gave my handlers notes that detailed the people I saw there so they would be able to identify the voices. I put in my notes to my handlers that I did this to record conversations where I was not physically present, and they never told me not to do this.

18. Malik told me more than once that he heard I was going regularly to *fajr*, or early morning prayer. He commended me on my commitment—he said that he had gotten into the routine of attending *fajr* prayers daily when he had been studying abroad, but that it was easy to fall back in attending prayers only when it was convenient and that he needed to get back to that kind of regimen. My handlers thought this was significant information that indicated Malik was returning to extremist beliefs, which justified further surveillance.

19. I gave significant information on Malik to my handlers. In addition to the surveillance described above, including giving my handlers recordings of all my conversations, my handlers several times showed me

photos with people they said had been seen with Malik and asked me to identify them. The pictures sometimes had Malik in them.

20. Malik was one of the individuals who my handlers told me were to be arrested in raids in about June 2007 that were ultimately aborted.

21. I never observed anything that gave me any reason to believe that Malik was involved in violence or terrorism in any way. I declare under penalty of perjury of the laws of the State of California and the United States that the foregoing is true and correct. Executed this [11]th day of October, 2010 in Los Angeles, California.

/s/ CRAIG F. MONTEILH
CRAIG F. MONTEILH

DECLARATION OF CRAIG F. MONTEILH

I, Craig F. Monteilh, make this declaration of my own personal knowledge and if called to testify, I could and would do so as follows:

1. From about July 2006 until about October 2007, I worked for the United States Federal Bureau of Investigation ("FBI") as an undercover informant assigned to infiltrate the Muslim community in Southern California. During this time, I generally spent about six or seven days a week posing as a Muslim convert named Farouk al-Aziz, conducting surveillance and gathering information on a wide variety of individuals and organizations in the Muslim community. My "handlers," or the FBI agents who directed my operations, during this time were FBI Special Agent Paul Allen and FBI Special Agent Kevin Armstrong.

2. On my handlers' instructions, I made audio recordings of everything I did while working as an informant, including all the conversations I had, using recording devices they had given me. I recorded all day, every day. My handlers told me that if something was not recorded, it was as if it didn't happen.

3. A few weeks after I publicly made a declaration of faith and started attending mosque, a group of young men approached me at mosque and, impressed that I was still attending mosque so regularly, told me that most of the group lived together and invited me to socialize with them at their house. My handlers were excited by this invitation. They told me that the home on Carver Street where the young men lived was already under surveillance because it was shared by five young, unmarried Muslim Egyptian men with different skills and backgrounds—including a computer analyst, a phar-

macist, an accountant, and one who handled logistics—and my handlers believed they might be a Muslim Brotherhood cell.

4. A few days after this invitation, I identified to my handlers that one of the young men who lived at the Carver street house, Yasser Abdel Rahim, was a person who seemed to attract and have influence with young Muslims. My handlers told me they thought Rahim was the leader of the cell, and that I should spend time at the Carver street house and with Rahim in particular, and gather as much information as I could. I did so, and recorded all the conversations I had with Rahim and the other members of the house. I gave these recordings to my handlers, along with notes about my observations.

5. My handlers instructed me to get into every room in the Carver street house to see what was in there, and include that information in my reports, which I did. Later, in about February or March of 2007, my handlers set me up with a video camera hidden in a shirt button and instructed me to conduct video surveillance of the layout and contents of the house, which I did.

6. On my handlers' instructions, I spent a lot of time at the Carver street house and with Rahim and his roommates. I never observed anything that gave me any reason to believe that Rahim or his roommates were involved in violence or terrorism in any way. They spent most of their time watching TV news (mostly Al-Jazeera), sports (football—bowl season, basketball, and soccer), talking politics, eating food, and playing X-box.

7. Shortly after I first met them, Rahim and one of his roommates bought me some books on Islam, and later asked me what I thought of them. Some time after that, Rahim agreed to meet with me weekly to teach me

various prayers. My handlers were excited by this because they thought Rahim was radicalizing me and would want me to be part of the Muslim Brotherhood. My handlers asked for the first sheet of paper on which Rahim had written a prayer for me to learn. When they gave it back to me a few days later, they told me they had lifted Rahim's fingerprints from it.

8. I informed my handlers that Rahim always led prayer in the house. This point interested them, because they said it showed leadership, and confirmed that I should focus surveillance on him.

9. My handlers said that Rahim had a criminal record, and they suspected he might be dealing drugs, but never suggested any particular evidence or investigation of narcotics activity, and I never observed any indication that any members of the house engaged in criminal activity.

10. I gathered and passed to my handlers information about Rahim's travel plans, particularly when Rahim was going to or from Egypt to see his family or his fiancé's family. After one of these trips to Egypt, Rahim complained that he had questioned for a long time when he re-entered the country—that he expected some delay but this had been way too long. I told one of my handlers this and he said, "'We're onto him," and indicated that they had been responsible for that questioning.

11. Rahim was very athletic. He played pick-up soccer with other Muslim youth. I attended some of these games and took down the license plates of people who attended, and once made a video recording with the hidden camera my handlers provided me, in order to docu-

ment who was attending and socializing with one another.

12. From my conversations with Yasser, I discovered that he traveled a lot to Portland for his job. I reported this information to my handlers, who were interested. They had a particular group of Muslims in Portland surveilled and believed he went there to report or get instructions from this group. I had a standing order to report all travel plans, and would find out Rahim's travel plans and tell my handlers. My handlers several times told me that they had Rahim surveilled in Portland after I had informed them he would be traveling there.

13. Rahim offered to introduce me to Sheikh Suhaib Webb, a white American religious scholar who studies in Cario. My handlers knew Webb and told me that although he portrayed himself as a moderate, he was an extremist, so they were very interested and instructed me to pursue this. Rahim gave me Webb's telephone number and email address, and my handlers told me to call or email Webb to make contact and establish a relationship, in hopes that Webb might give me some instructions. I called his cell phone and talked to a family member and emailed with him, but my operation ended before I met him.

14. Rahim's fiancée lived in Detroit. I talked to Rahim about her and her family, and transmitted what information I learned to my handlers. I also got her email address from emails he had forwarded that came from her, and passed that on to my handlers. My handlers were suspicious of his fiancé's family because they were prominent people who traveled to Egypt often.

They later told me his fiancé's family in Detroit was under surveillance as well.

15. On different occasions, my handlers told me that the FBI had electronic listening devices in the house, as well as in Rahim's car and phone. For example, one day, one of my handlers called to tell me that a friend had driven up to the house quickly in an agitated state and asked me to go down there to find out what was going on. When I asked how he knew this, he indicated they had video outside the house. Another time, my handlers asked me about something that happened inside the house that I hadn't yet put in my notes. I asked how they knew, and they told me that they had audio surveillance in the home.

16. My handlers told me that Rahim was donating money to a charitable organization in Egypt. They told me that these donations had been tracked by the Treasury Department. They told me that these donations were not unlawful, but that they could make them seem suspicious in order to threaten him and pressure him to provide information and become an informant.

17. On many Tuesday nights, the imam from the Garden Grove mosque, Mustafa Kamil, would give Arabic language teachings at the Islamic Center of Irvine. Rahim often attended. On several occasions, I used recording devices provided to me by my handlers to record these teachings and the discussions after. On these occasions, I went into the prayer hall and listened to some of the teaching. Since I did not want to arouse suspicion by staying when I was just starting to learn Arabic, I would leave my things—including the recording device (disguised as a key fob or cell phone)—near to where the group was talking, and then go to another part of the

mosque or a different part of the prayer hall to pray. My recording device would capture their conversation when they did not think I could hear. Rahim was part of the group I recorded on several occasions.

18. On my handlers instructions, I asked Rahim questions about jihad and pressed him on his views about religious matters and certain religious scholars, particularly Egyptian ones, in order to get him to say something that might be incriminating or provide a way to pressure him to provide information to the FBI. Rahim told me that there was more to Islam than jihad: that jihad is a personal struggle, and that to the extent that there is such thing as a fighting jihad, the Quran places very strict rules that prohibit harming plants or trees, infants, elderly or women, and that terrorists who say they are engaged in jihad are not, they are just committing murder. When I asked about religious scholars like Hassan al-Banna and Sayid Qutb, who my handlers told me to ask about because they are considered extremist, he said that he did not agree with them, but thought that the Egyptian government should not have executed them.

19. Rahim was one of the individuals who my handlers told me was to be arrested in the aborted raids of June 2007.

I declare under penalty of perjury of the laws of the State of California and the United States that the foregoing is true and correct. Executed this [11]th day of August, 2010 in Orange, California.

/s/ CRAIG F. MONTEILH
CRAIG F. MONTEILH

APPENDIX I

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Nos. 12-56867, 12-56874, 13-55017

YASSIR FAZAGA, ET AL., PLAINTIFFS-APPELLANTS

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL.,
DEFENDANTS-APPELLEES

Filed: June 25, 2015

MOTION FOR LEAVE TO FILE SUPERSEDING BRIEFS

The federal defendants-appellees (the Federal Bureau of Investigation and two FBI employees in their official capacities) hereby move for leave to file superseding unclassified and classified briefs, to account for the declassification of information that was previously included in the government's classified brief. * * * *

* * * * *

2. Plaintiffs filed their opening brief on November 17, 2014. On March 17, 2015, the government filed a public brief as appellee containing the information and legal argument that could be filed on the public record. On the same date, the government filed, *ex parte*, a classified brief and classified excerpts of record, each of

which contains classified information that was filed in the district court. Plaintiffs sought reconsideration of this Court's order granting leave to file a classified brief, and this Court referred plaintiffs' motion to the merits panel, but directed that the classified brief be provisionally maintained on an *ex parte* basis pending resolution of the motion. Order, May 12, 2015.

On April 29, 2015, the individual defendants filed their briefs as appellees/cross-appellants. Plaintiffs' response/reply brief is currently due July 23, 2015.

3. Several months after the government's brief was filed, the FBI declassified a single paragraph of the Classified Declaration of Mark Giuliano, which had previously been classified at the Secret level. The declassified information relates to the agreement entered into between the FBI and Craig Monteilh, the confidential informant whose conduct is at issue in this case, regarding the use of recording equipment. The declassified paragraph is attached to this motion, along with an exhibit that is referenced in the declassified paragraph.

The declassified paragraph does not contain information as to which the government has ever asserted the state secrets privilege in this case, as it does not "tend to confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation," does not "tend to reveal the initial reasons . . . for an FBI counterterrorism investigation of a particular person . . . , any information obtained during the course of such an investigation, and the status and results of the investigation"; and does not "tend to reveal whether particular sources and methods were used in a counterterrorism investigation of a particular subject." Holder Decl. ¶ 4 [ER 285]. To the contrary, the

now-declassified paragraph of Mr. Giuliano's declaration expressly contemplated that this information would be subject to declassification review. *See* Classified Giuliano Decl. ¶ 22 (attached) ("[W]ith respect to plaintiffs' specific assertion that the FBI acquiesced in Monteilh's leaving recording devices unattended inside mosques, the FBI is assessing whether specific instructions to Monteilh concerning this particular 'unattended device' issue can be disclosed without harm to national security.").

Because we filed our appellate brief at a time when the now-declassified paragraph was classified at the Secret level, the information in that paragraph was omitted from our public filing, and instead discussed in two sentences of our classified filing. To clarify the record for the parties and the Court, and to provide the Court with a current and accurate representation of which information is classified and which has been publicly disclosed, we respectfully request leave to file superseding briefs. The only changes are the insertion of the declassified information into the public brief, and the removal of that information from the classified brief (along with conforming changes to the tables and certificates).

We have attached to this filing a redline version of the single page of the public brief that has been changed. We are also attaching to this filing a complete version of the superseding public brief that we seek leave to file. If the Court grants this motion, we will file a superseding classified brief under appropriate procedures. The classified brief will be modified only by deleting the two sentences containing the information that is now included in the superseding public brief.

* * * * *

For the foregoing reasons, we respectfully request that this Court grant leave to file superseding public and classified briefs.

Respectfully submitted,

/s/ DANIEL TENNY
DOUGLAS N. LETTER
DANIEL TENNY
Attorneys
Civil Division, Room 7215
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001
(202) 514-1838

JUNE 2015

ATTACHMENT 1
DECLASSIFIED MATERIALS

Declassified Paragraph of Giuliano Declaration

22. In addition, with respect to plaintiffs' specific assertion that the FBI acquiesced in Monteilh's leaving recording devices unattended inside mosques, the FBI is assessing whether specific instructions to Monteilh concerning this particular "unattended device" issue can be disclosed without harm to national security. The FBI can advise the Court at this stage that Monteilh agreed in writing to keep FBI issued recording devices with him at all times while they were turned on. He executed the attached FBI form FD-473 on November 17, 2006 (attached at Tab 6) which states in pertinent part:

> I, Craig Monteilh, hereby authorize members of SARA 6 and Special Agents of the Federal Bureau of Investigation, United States Department of Justice, to place a Body Recorder on my person for the purpose of recording any conversations with various CT [subjects] and others yet unknown which I may have on or about 11/17/06 and continuing thereafter until such time as either I revoke my permission or the FBI terminates the investigation.
>
> I have given this permission to the above-named Special Agents voluntarily and without threats or promises of any kind. I understand that I must be a party to any conversation in order to record that conversation. I therefore agree not to leave the recording equipment unattended or take any other action which is likely to result in the recording of conversations to which I am not a party.

[PAGE INTENTIONALLY LEFT BLANK]

[FOLDOUT]

FD-473 (Rev. 6-1-00)

11/17/06
(Date)

Santa Ana, CA
(Location)

I, CRAIG MONTEILH,
(Name)

_____,
(Address)

hereby authorize members of SARA C and

_____, Special Agents

of the Federal Bureau of Investigation, United States Department of Justice, to place a

☒ Body Recorder

on my person for the purpose of recording any conversations

☐ Transmitter

with various CT
(Name of Subject(s))

and others as yet unknown which I may have on or about 11/17/06 and
(Date)

continuing thereafter until such time as either I revoke my permission or the FBI terminates the investigation.

I have given this written permission to the above-named Special Agents voluntarily and without threats or promises of any kind. I understand that I must be a party to any conversation in order to record that conversation. I therefore agree not to leave the recording equipment unattended or take any other action which is likely to result in the recording of conversations to which I am not a party.

_____
(Signature)

Witnesses:

_____

_____

APPENDIX J

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

SACV 8:11-cv-00301-DOC

YASSIR FAZAGA, ET AL., PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL., DEFENDANTS

Monday, July 14, 2025
1:21 P.M.

REPORTER'S TRANSCRIPT OF PROCEEDINGS

APPEARANCES OF COUNSEL:

FOR THE PLAINTIFF, YASSIR FAZAGA, ET AL.:

AHILAN T. ARULANANTHAM
UCLA School of Law
385 Charles E. Young Drive East
Box 951476
Los Angeles, California 90095
(310) 825-1029
arulanantham@law.ucla.edu

MOHAMMAD K. TAJSAR
ACLU Foundation of Southern California
1313 West 8th Street
Los Angeles, California 90017
(213) 977-5200
mtajsar@aclusocal.org

FOR THE DEFENDANT, FEDERAL BUREAU OF INVESTIGATION, ET AL.:

JULIA A. HEIMAN
U.S. Department of Justice
Civil Division—Federal Programs Branch
1100 L Street NW
Washington, DC 20005
(202) 616-8480
julia.heiman@usdoj.gov

ALEXANDER H. COTE
Scheper Kim & Harris LLP
800 West Sixth Street
18th Floor
Los Angeles, California 90017
(213) 613-4655
ACote@winston.com

* * * * *

[7]

THE COURT: Okay. The case was with Judge Carney. It's being re-assigned to my court. So let's talk about some of the folks that come from this letter. And, first of all, eventually, I'm going to ask you: How do I even [8] substantiate that this letter is from Craig Monteilh?

So when you respond to the Court—I've got a hearsay letter unsigned. What do I do with that, in terms of making an evaluation of how the Court proceeds, depending upon your different viewpoints of when it should be decided?

The second thing is, I don't think I know any of the characters in this letter, or gentlemen, but I do represent to you that I've been to Afghanistan at least 15 times, and I've been involved with Dostum, who's your northern warlord and former president. But in reading this letter, I don't know Gulbuddin Hekmatyar—at least I have never met him—nor do I know Amin al-Haq, but I certainly know who they are. And in representing to you, without going too far, I've been there on a number of occasions doing rule of law projects with judges in Afghanistan. And through those relationships in Kabul, Mazar-i-Sharif, Barak, I've meet most of their judiciary. That on some cases has translated over into meetings—I'm giving you full disclosure in case anybody is uncomfortable—that is translated over into various meetings with the former department of their justice system.

* * * * *

[13]

Now, if that causes you discomfort in any way, I think I've disclosed as fully as I can, you know, those trips I've taken. And one of the tragedies is we've had to leave a number of the women and males subject to the Taliban. A couple of them have been murdered, by the way.

[14]

Now, I want you to have a discussion. If any of you are uncomfortable having me preside over the case, let

me know right away. Otherwise, we're off and running. Go have a talk with each other. Good-bye. That's an order. Go out in the hallway.

Now, there might be a little bit more. I probably disclosed too much. And by the way, any conference without Kandahar is not a good conference.

And one funny story to leave you with, my first time over, I have 150 Afghan Judges. I asked the question, *How many of you are taking a bribe?* Not one hand goes up. My next question is *How many of you know of another judge taking a bribe?* 60 percent of the hands went up. Go out and have a good conference, okay?

And by the way, I'm not affronted. If you want me off the case, no problem. Otherwise, let's get the case rolling, okay.

You look like you're lost.

MR. MONTEILH: No, sir. The letter in front of you. The seven page—

THE COURT: I can't—oh, you are?

Well, have a seat. I don't want to talk to you. I may want to talk to you in just a moment, okay? But not right now. Not without counsel. Just sit and listen.

(Pause.)

[15]

THE COURT: I'm not affronted either way. Do you want to continue on in this court or are you in any way uncomfortable?

And the only reason I made that disclosure is I don't know where this goes, eventually, and I'd hate to have some witness come in—it's certainly not going to be

Haq, not some of these other characters. But I just want to make sure that I don't have a situation where a court might get caught, you know, six months from now or whatever and here comes a witness who I've might have seen. There's been a number of other meetings, obviously. I just don't care to go there, but I think that's enough of a disclosure to give you kind of an idea how close I've been to that country and a lot of the leaders there.

Do you want me stay on the case, or do you want to get rid of it?

MS. HEIMAN: Your Honor, I'll start out, on behalf of the Government defendants, I don't anticipate any issues. The only thing I would add is that if the Court might give me an opportunity to confer with my leadership just to make sure.

THE COURT: Absolutely.

MS. HEIMAN: I would appreciate it.

THE COURT: And the leadership—I may—depending upon who it is, I wonder if I've been in some way [16] involved with your leadership. First is if Mueller is on the line. Mueller was in the Marine Corps with me, okay? You know that the FBI blew the whistle on the CIA concerning the torture chambers of Bagram. Our own country straightened that out. You got Mueller coming in here. I'd like to disclose that to the plaintiffs that I have a personal relationship with him. You should know that. That's what I'm concerned about. That's why I'm over-disclosing and in some ways I'm under-disclosing, okay? And if there's any discomfort, don't worry about that. We've got 29 other judges, okay? But, otherwise,

you got a fascinating case, I'm telling you. You've got an amazing case.

And I think the last time I saw you was on the MEK, wasn't it?

MR. COTE: It was, Your Honor.

THE COURT: And all of you worked all night, which was exemplary and brought me pleasure the next day, which I didn't expect. So I've had a prior relationship with counsel on an MEK case that you should know about, okay?

So do you want get rid of me, or do you want to keep me? Either way is fine.

MR. ARULANANTHAM: No, Your Honor, we don't want to get rid of you. We don't see any basis to—

THE COURT: Then, could we tentatively continue [17] today so I'm not wasting your time, but get back to me in the next day or so in case there's a problem.

Now, the gentleman right here—sir, would you stand up again with no disrespect. The gentleman in the back. No, that guy.

Come on up here for just a moment.

He started to identify himself to me. And I immediately cut him off, and I didn't mean to be rude.

But, sir, your name is?

MR. MONTEILH: Craig Monteilh.

THE COURT: Yeah. So I immediately said, *Sir, would you have a seat. Counsel is in the hallway.*

So, sir, with no disrespect, would you, please, have a seat again. So he's present.

Well, what are your thoughts about this case? How should we proceed, because Judge Carney has had this a long time. It seems to have quite a—quite a history.

MR. ARULANANTHAM: Your Honor, I think as to the question of what to do with the letters and how to proceed more generally, you know, our view is that at this point, we should wait to see if the Government seeks cert from the Supreme Court. You know, we—last time we actually were taking more or less—"last time," meaning after we won on appeal in the Ninth Circuit, before the Supreme Court took it the first time, we were kind of in a sense in mirror [18] images positions. We said we should go forward on the portions of the case that should go forward without—that are not subject to the state secrets privilege, you know, on their view. And they said, *Well, we're not sure exactly what scope of the case will or will not be subject to the privilege.*

They won on that question. We went to the Supreme Court and the Supreme Court's order changed the scope of the case, substantially. It, essentially, got rid of the FISA, except for our 1810 claim which is still in this case. It got rid of the extent to which FISA could ameliorate the state secrets privilege and the case came back to the Ninth Circuit, obviously, and then we won again. And now we're here.

And my view is, you know, we could do various things between now and August 13th, or—which is—their deadline is August 13th to seek cert or not. But a lot of what we do—a lot of the things that we would like to do next in the case could be substantially impacted by a Supreme Court order and it could, potentially, radically change the scope of the case, you know, either entirely knock

out the religious discrimination aspects of the case, which is what the Government's position is, or not.

And so it just seems to me like it doesn't make sense to proceed now until we know. You know, we might know [19] as soon as August 13th. Then I'm happy to tell you our thoughts about what we—Your Honor, what thoughts we might have about what to do then. In our view, the threshold issue is we should just wait and see if we're going to the Supreme Court or not.

THE COURT: The Government has a different viewpoint.

I know you would like to proceed. So what are your thoughts?

MS. HEIMAN: Yes, Your Honor.

And the reason the Government would like to proceed is that this case is based foundationally on the prior declarations of Mr. Monteilh. There were four declarations submitted alongside the plaintiff's opposition to the Government's prior dispositive motions. And our position is that regardless of what happens with further appellate process, the whole—the crux of the case factually, it really is fairly straightforward. Is it the case that the FBI, as Mr. Monteilh previously stated, was surveilling people solely on the basis of their religion, or not?

The only evidence in the case that there was for that was Mr. Monteilh's statements. In light of his recent statements—and I'll add, Your Honor, that we received another letter—we and plaintiff's counsel received [20] another letter from Mr. Monteilh, on Friday, reiterating his positions from the letter that we submitted that his allegations weren't true.

We submit, Your Honor, that the Court should first test and fact find as to that very foundational premise, and it may affect what happens on review as well.

So our position is we'd very much like to forge ahead, and we think it appropriate for the plaintiffs to submit a response. Regardless of whether the Court orders a response, our proposal would be that the Government submit a motion to strike the prior declarations and there could be proceedings on that notice motion going from there.

THE COURT: I opened this session by a concern about the foundation of this letter. The gentleman is literally here. One of the things that I can accomplish very quickly is clearing up my record and putting him under oath for one minute and saying, *Basically, did you write this letter?*

And I would like to do that so I have a record, because right now, I'm not certain in an unsigned letter what I'm dealing with.

Would that be acceptable if I just ask that one question and clear up the foundation?

MS. HEIMAN: I'm sorry to interrupt, Your Honor. If I may—yes, the Government would concur with that. No [21] objection.

And, also, Your Honor, I have with me an unredacted, because what we filed on the docket to protect people's privacy was redacted. I have clean copies. And Mr. Monteilh sent two follow-up missives: One, which the plaintiffs added to our joint status report also in redacted form and then the Friday submission.

So if I could provide those to the Court after showing counsel, then all three could be—

THE COURT: All I need today is—I don't intend to conduct a hearing today, unless each of you want that. But I would like to get at least a foundation that these letters are, in fact, from the gentleman, because they are unsigned. They're hearsay at the present, so I think if I could simply go into what I'm going to refer to as the "Operation Flex" letter. It doesn't have a date on it. It just begins "Dear Distinguished Attorneys for Plaintiffs and Defendants." And then to whatever other documents you may have that are signed or unsigned in the meantime, that would save us a lot of time in the future.

MR. ARULANANTHAM: Your Honor, I'll just make two points about it: First, this is at the motion-to-dismiss stage. We filed those declarations just to affirm that the allegations in the complaint were plausible which is all that we need to establish as you know, of course, under [22] *Iqbal*. So even if there were a recantation—and I'm not saying, you know, we shouldn't establish the authenticity of the letters. But even if there were an actual recantation to everything in the declarations, which is not what the letters say, it wouldn't change the fact that the allegations are plausible.

THE COURT: It may not. That's—I understand that. That's for argument later.

MR. ARULANANTHAM: Right.

THE COURT: I just don't know what I'm dealing with, because it was submitted—thank you—by the plaintiffs. By the same token if I later hear that this is irrelevant, depending upon my ruling, et cetera, what do I do with that?

I've got the gentleman here. It's easy to verify.

Sir, would you be kind enough to come up again—and pardon our discourtesy—just come to the lectern for a moment.

(Pause.)

THE COURT: And the lectern is right there *(indicating)*. I don't even have to have you take the witness stand.

Would you raise your right hand, sir.

Karlen, my clerk, she's going to administer an oath to you.

[23]

CRAIG MONTEILH, WITNESS, SWORN

THE WITNESS: Yes.

THE COURT: Thank you very much, sir.

Sir, I'm going to give you, actually, my copy and disregard all the yellow underlining on it. That's my underlining when I am reading it. Take a moment and look at that copy for just a moment.

And, Counsel, each of you can look at it. Don't worry about the yellow underlining.

THE WITNESS: One moment, sir. I'm looking for my glasses.

(Pause.)

THE CLERK: Can I have your name for the record?

THE COURT: Oh, just a moment, Karlen. We'll get it.

(Pause.)

THE COURT: It's about four pages, maybe five.

(Pause.)

THE COURT: First of all, your name?

THE WITNESS: Craig Monteilh.

THE COURT: And could you spell your last name, sir?

THE WITNESS: M-O-N-T-E-I-L-H.

THE COURT: Are you author of that letter, sir?

THE WITNESS: Yes, sir.

[24]

THE COURT: Okay. Now, do you have some additional letters?

So I don't have to call the gentleman back, because I don't know if they are signed or unsigned. I've never seen these other letters.

MS. HEIMAN: Yes, Your Honor.

I have copies of the statements that Mr. Monteilh sent to us and to plaintiffs' counsel over the last—there have been three such letters.

THE COURT: Well, let's refer to this as Exhibit 1.

And could you give me a copy that's clean? One of the parties—

MS. HEIMAN: Yes, Your Honor.

THE COURT: —to give to Karlen right now so we can start a good record.

And then, sir, if you would give me back my copy for just a moment to Karlen. We're going to hand you another letter.

We'll going to call it Exhibit 2, and we're going to identify it in some way.

(Pause.)

THE COURT: Both counsel are welcome, informally, to get up at any time and just gather around the lectern to see what he's looking at.

[25]

MS. HEIMAN: When the Court is ready, I have a third as well.

THE COURT: Let's just take Exhibit 2 for a moment.

(Pause.)

THE COURT: I'll also represent to you, I was in Pakistan when Osama bin Laden was killed. I had no advance notice of that, other than the ambassador telling me that something was going to happen that would change the war on terror at a social function, on Friday night, asking when I would fly out. I flew out at 3:00 a.m in the morning. Osama bin Laden had been killed at about 1:30 by the SEAL Team, so I represent to you I had no advance notice of that operation, nor in reading these quickly do I have any recollection of having ever met any of the FBI agents named in these documents.

So do you have a copy of this in front of you, sir?

THE WITNESS: Which one, Your Honor?

THE COURT: It's the second. We're going to call it *(Reading)*:

"Operation Flex, Information Classified and Privileged, Fazaga versus FBI. Dear Distinguished Attorneys for Plaintiffs and Defendants."

[26]

So this letter starts the same way, sir, as the second one. And we should put that letter in front of you, and mark it maybe "2" at the top. No. 2, okay?

Can somebody do that for the gentleman?

(Court's Exhibit 2 received in evidence.)

MS. HEIMAN: Forgive me, Your Honor. This is the one that starts: "Clarification and verification"?

THE COURT: No, I don't have that one. I've got "Dear Distinguished."

I just have a copy of the—Karlen, this is going to be Exhibit 1 *(indicating)*. This will be Exhibit 2 *(indicating)*. That's what I don't have. I do now.

So I want both of you to mark that in each others' presence and verify that this is Exhibit 2, the same document.

THE CLERK: This is 1?

THE COURT: That's 1. Put No. 1 on it. It's received into evidence.

(Court's Exhibit 1 received in evidence.)

THE COURT: No. 2 starts: "Clarification and Verification."

MR. ARULANANTHAM: No, Your Honor.

THE COURT: Remember, in the first document you gave me, all that information was redacted, so I'm not

seeing any of the agents. I may have met CIA or FBI. Now, [27] I'm seeing that in that document.

I represent to you, I don't know any of those folks.

MR. TAJSAR: Your Honor, just a clarification. So that what you just referenced as No. 2 is in fact No. 3.

THE COURT: Okay. Time out. Give me No. 2.

MR. TAJSAR: This is No. 2 *(indicating)*.

THE COURT: We'll go by the numbers here. Okay. No. 2.

MR. TAJSAR: That's No. 2.

THE COURT: Thank you.

In addition to the Government's filing of June 30th, 2025.

Sir, do you have that document in front of you?

THE WITNESS: I do, Your Honor. Yes.

THE COURT: Could we mark that No. 2 at the top. Would you help the gentleman? No. 2.

(Court's Exhibit 2 was marked for identification.)

Now, let me read this and you read it also, sir, to yourself.

(Pause.)

THE COURT: By the way, one of the reasons that Robert O'Brien and I talked is we wanted this program on behalf of young people in Afghanistan, male and female, to continue, regardless of which administration was in power. [28] We were very worried that Condoleezza Rice might start it and Hillary Clinton might pick it up. And we needed to make certain if our Government was

going to make that kind of matter. It didn't matter who the president or administration was. So we tried to balance that out with, let's say, some balance.

I represent to you I don't know any of the general counsel involved. I don't recognize them and I don't recognize any of the agents, et cetera.

Sir, did you write this letter?

THE WITNESS: I have a problem, sir.

THE COURT: Okay.

THE WITNESS: And the problem that I'm facing is this: I understand—

THE COURT: Let me be very clear. I don't want to get into a discussion with you today. It's discourteous to you.

My questions are really simple to know what I can take as relevant information or not. Right now, it's hearsay.

Did you write this letter?

THE WITNESS: Yes, sir.

THE COURT: Okay. That's real simple.

Received as Exhibit 2. Would you mark that.

(Court's Exhibit 2 received in evidence.)

[29]

THE COURT: We're going to give you something called "Clarification and Verification." And we're going to mark that Exhibit 3.

(Court's Exhibit 3 was marked for identification.)

THE COURT: And do you have that in front of you, sir?

THE WITNESS: I do.

THE COURT: And is it marked "Exhibit 3" at the top?

THE WITNESS: I do, yes.

THE COURT: Okay. Thank you very much, sir.

(Pause.)

THE COURT: Sir, have I ever met you before?

THE WITNESS: I don't believe so, sir.

THE COURT: The only name that I recognize in this document that I have had contact with would be Deirdre Eliot, who was a former prosecutor for the United States Government in a number of cases in my court 10 years ago or so. Beyond that, I don't recognize—

Sir, did you write the "Clarification and Verification?"

THE WITNESS: Yes, Your Honor, I did.

THE COURT: Okay. Thank you. Was there a fourth document?

MS. HEIMAN: Not from us, Your Honor.

[30]

THE COURT: Sir, thank you very much for your courtesy. I appreciate it. That's all I needed today.

If you want to remain, you're more than welcome to. One of the issues may become any accusations made against you or members of the plaintiff's team. I would tentatively not find any conflict in that regard. In other

words, this is not going to cause a removal of you as a representative of the plaintiffs in this matter and, therefore, it may be a situation where you're testifying literally or casting an affidavit. The second thing is I need you to make a phone call. I don't want to start making rulings and then if I'm in favor or ruling in favor or against anyone, *Judge, you know, we thought about it, and we'd like you to remove yourself.*

Could you go make those phone calls; and if not, could we come back tomorrow?

MS. HEIMAN: Absolutely.

THE COURT: Take your time with it. I just don't want to get further down the line. So if there's any uncomfortableness trust me, I've got 400 cases, okay? Nice seeing all of you. But if not, then I would like to really start setting some wheels and parameters to whatever we think we're going to do, whether it's a stay or proceeding forward. And I don't want to start making those rulings and then have one of you decide, okay?

[31]

MR. ARULANANTHAM: Just one brief thing in that regard, Your Honor. You said you knew Robert Mueller. It's not inconceivable that he could testify in the case, but I assume that would—

THE COURT: I don't know him well. He was—I was two classes ahead of him in Marine Corps Officer Candidate School. I was with the unit called the "Walking Dead" in Vietnam. He was also a second lieutenant, two behind me, along with Kelly, along with Jim Mattis. So I have met him in D.C. on an unrelated case, in terms of a plea bargain, that I don't want to go any further with, and persuading his government—his office to take an-

other look. It worked out well for both parties. That's all I'll say. But it required a personal trip back to D.C., literally, at the request of your office and the defense to go back and talk to his second-in-command about reevaluating. And both sides came away pretty happy.

I met with his chief of staff, Grant something. So I at the time said, "Hi." We have a lot of mutual friends. And I saw him at a state department function, briefly, when Ghani was brought over to the United States in terms of some foreign aid issues that we had with Afghanistan, okay? But I haven't seen him in 10 years.

Okay. Why don't you go make that call, okay?

MS. HEIMAN: Yes, Your Honor.

[32]

THE COURT: And we'll be here waiting, because if we're still on the case, then we'll get rolling, okay?

(Pause.)

THE COURT: Counsel, I'm going to stay out of session so I'm not moving the Holloway matter back into session and then moving you out again. That could probably be a quick call.

Do you have to call D.C.?

MS. HEIMAN: Yes, Your Honor.

THE COURT: It's almost 5:00 o'clock. Let's go see if they're still working.

MS. HEIMAN: I have cell phones.

Counsel, let's stick around for a moment. I'm going to take a recess. I want you to remain seated, because I keep moving people in and out, and it's inconvenient.

(Pause.)

THE COURT: Thank you, counsel, for your courtesy. I appreciate it. We're back on the record.

Counsel, were you able to place that call?

MS. HEIMAN: Yes, Your Honor. And I can confirm I got the green light.

THE COURT: Which means it's okay to stay on the case then, okay?

All right. Let me retrace then a couple thoughts. [33] I'm going to summarize what I think the Ninth Circuit has—opinion says and then correct me and add to it, okay?

I think the issue before this Court is going to be whether plaintiff's religious claims may proceed or if they should be dismissed at the pleading stage, based on the state secrets privilege properly invoked by the Government under *United States versus Reynolds*.

And based on the decisions of the Supreme Court and the Ninth Circuit, this Court was instructed to conduct a detailed and fact intensive examination of whether the privilege evidence mandates dismissal under the exceptional circumstances recognized in the *Jeppesen Dataplan* case, rather than merely the exclusion of the evidence.

Two exceptional circumstances may necessitate the rare dismissal of the claims, rather than exclusion: First, if the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim. And under these circumstances, the Ninth Circuit has said, quote: "The District Court may properly dismiss the complaint only if it conducts

an appropriately tailored *in camera* review of the privileged record and determines that defendants have a legally meritorious defense that prevents recovery by plaintiffs."

Because the Court is considering evidence beyond the pleadings, plaintiffs must be given an opportunity to [34] prove a *prima facie* case without privileged information and refute defendants' defenses. This procedure melds summary judgment procedures with an expanded nontransparent fact-finding rule for judges.

Second, if it is possible to proceed with the litigation—I'm sorry. If it is impossible to proceed with the litigation because privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses, litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets.

The Ninth Circuit has said, quote:

> "In rare instances in which the risk of disclosure cannot be averted through the protective measures routinely used by courts, the case must be dismissed, leaving the plaintiff without a remedy for a possibly meritorious claim," end of quote.

The Ninth Circuit instructed the District Court to consider all possible protected measures and highlighted that substantial information has already been made public and that is—and that this decades-long litigation has not resulted in proper disclosure so far.

So, Counsel, if you have anything further you'd [35] like to comment upon this, and then I think I'll make the ruling concerning this first issue in front of you, okay?

MR. ARULANANTHAM: The only thing I would—

(Court Reporter requests clarification for the record.)

MR. ARULANANTHAM: The only thing I would add, Your Honor, is that in footnote 20 of the opinion, they note that there is a large body substantial, or something like that, where they use body of information, not privileged, which the Government has said they think should be made available in the proceeding in this case.

THE COURT: Counsel.

MS. HEIMAN: Yes, Your Honor. Thank you.

So the very foundation of the Ninth Circuit's decision, in 2024, was that the Court understood that plaintiffs could make their *prima facie* case without reliance on classified evidence. That's in Footnote 8 of the Court's decision. And, indeed, that's found in the plaintiffs' previously submitted pleadings where they cite Mr. Monteilh's declarations. And that factual predicate, the idea that plaintiffs can make their case without reliance on classified discovery, that's now shaken and, in the Government's view, requires exploration in the first instance before we get into potential proceedings under the Ninth Circuit's subsequent instruction.

[36]

This all rests on the assumption that plaintiffs were presiding with Mr. Monteilh's declaration. So we would urge the Court to allow the Government to proceed on the motion to strike and to explore those issues first.

THE COURT: Counsel, I'm going to grant the very limited stay that the plaintiffs are requesting in this matter. The deadline—the Government's deadline to decide whether they are seeking certiorari with the Su-

preme Court is August 13th, 2025. I believe it's inefficient—that it is efficient to wait that one month until and before I decide the issue of how the case will proceed. In particular, the Government is asking the Court to test the sufficiency of the allegations in the case and get into evidence that the Court usually does not address at the pleading stage. To do this, I think, would be very unusual, and I don't believe it's appropriate particularly when this may be taken up by the Supreme Court and drastically changed. In addition to that, I'm just not sure how I would accomplish that.

I leave literally tomorrow afternoon for Saipan for designation for two weeks. That has nothing to do with the ruling. I'm just saying we would be scrambling, but I would make a record. That has nothing to do with this. I can probably do this from Saipan and video conference. I choose not to. I think it's much more efficient, and I [37] think it will proceed in a much more orderly fashion. Now, that doesn't preclude future motions on this regard. Let's see what the Supreme Court does first. Let's see what your decision is at this point, okay?

When do I set a next tickler date? Would I set it early September for you, after we decide whether you're going to take a writ of certiorari to the Supreme Court? In other words, get your calendar. Be kind to each other. I'm here all the time. Give me some suggested dates.
* * * *

* * * * *

APPENDIX K

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

Case No. 8:11-cv-00301-DOC-VBK

YASSIR FAZAGA, ET AL.

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL.

Filed: July 14, 2025

CIVIL MINUTES—GENERAL

Present: The Honorable DAVID O. CARTER, United States District Judge

ATTORNEYS PRESENT FOR PLAINTIFF:

MOHAMMAD TAJSAR

ATTORNEYS PRESENT FOR DEFENDANT:

JULIE HEIMAN
ALEXANDER COTE

PROCEEDINGS: STATUS CONFERENCE

The Case is called. The Court and counsel confer.

The Court STAYS proceedings pending the government's decision to seek Supreme Court review of the Ninth Circuit's decision.

The Parties shall file a joint status report by August 14, 2025.

: 52
Initials of Deputy Clerk: kdu

APPENDIX L

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

Case No. 8:11-cv-00301-DOC-VBK

YASSIR FAZAGA, ET AL.

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL.

Filed: Aug. 20 2025

CIVIL MINUTES—GENERAL

Present: The Honorable DAVID O. CARTER, Judge

ATTORNEYS PRESENT FOR PLAINTIFF:
None Present

ATTORNEYS PRESENT FOR DEFENDANT:
None Present

PROCEEDINGS (IN CHAMBERS):

ORDER MAINTAINING STAY AND ORDERING JOINT STATUS REPORT BY OCTOBER 15, 2025

Based on the Joint Status Report (Dkt. 203) submitted by the Parties on August 14, 2025, the Court maintains the present stay in this case pending the Government's decision to seek Supreme Court review of the Ninth Circuit decision. Because the Government's deadline to file a petition for review with the Supreme Court

has been extended to October 10, 2025, the Court hereby orders that the Parties submit a joint status report by October 15, 2025.

The Clerk shall serve this minute order on the parties.

MINUTES FORM 11 Initials of Deputy Clerk: kdu

CIVIL-GEN

APPENDIX M

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

No. CV 8:11-cv-00301-DOC-VBK

YASSIR FAZAGA, ET AL., PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL., DEFENDANTS

Filed: Sept. 4, 2025

GOVERNMENT DEFENDANTS' NOTICE OF FILING OF STATEMENTS OF CRAIG MONTEILH

Defendants the United States of America, Federal Bureau of Investigation, and all Government Defendants sued in their official capacity (collectively "Government Defendants") respectfully submit this notice of filing the recent statements of Mr. Craig Monteilh.

At the July 14, 2025, status conference, the Court admitted into the record as authentic the following three statements of Mr. Monteilh, upon Mr. Monteilh's in-court verification under oath as to their authenticity:

Exhibit 1: June 10, 2025, Statement

Exhibit 2: July 4, 2025, Statement

Exhibit 3: July 11, 2025, Statement

A true and correct copy of each of those statements is attached hereto, as Exhibits 1, 2, and 3, respectively.

Also appended hereto as Appendix A is the declaration of undersigned counsel, supplying true and correct copies of Mr. Monteilh's emails transmitting Exhibits 1, 2, and 3.

Dated: September 4, 2025

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General

JEAN LIN
Special Litigation Counsel

/s/ JULIA A. HEIMAN

JULIA A. HEIMAN
Senior Counsel
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, NW
Washington, D.C. 20530
Telephone: (202) 616-8480/
Fax: (202) 307-0442
E-mail: julia.heiman@usdoj.gov

Attorneys for the Government Defendants

Exhibit A-1

Heiman, Julia (CIV)

From:	Craig Monteilh [**REDACTED**]@yahoo.com>
Sent:	Tuesday, June 10, 2025 9:06 PM
To:	Hinshelwood, Bradley A. (CIV); Slade, Scooter (JMD); Trevor Aaronson
Cc:	Ahilan Arulanantham; [**REDACTED**]@aclusocal.org; Hussain, Suhauna; Heiman, Julia (CIV)
Subject:	[EXTERNAL] Operation Flex/Fazaga v FBI
Attachments:	Operation FlexFazaga v FBI.pdf

Please carefully read the attached.

Exhibit 1

OPERATION FLEX
Information Classified and Privileged
(Fazaga v FBI)

Dear distinguished attorneys for Plaintiffs/Defendants,

I, Craig F. Monteilh, created the idea of Operation Flex in May 2006. I pitched the idea of infiltrating mosques to 4 FBI agents at different times. The agents were SA's Tracy Hanlon, Christopher Gicking, Kevin Armstrong and Paul Allen.

I have a history of creating operations dating back to 1983, at age 21. I can corroborate this with the attached newspaper article by *The San Gabriel Valley Tribune.* Please be advised, I was not properly vetted for the operation. The idea was unique and sound. The agents heard it, liked it and immediately sought to fund it. I was white, a very muscular man with a powerful build, very street smart (ex-convict) and an unmatched knowledge of geopolitics. Those are the unique qualifications of an intelligence expert operating in the field.

Having stated the above, I have created 2 very important lawsuits. The lawsuits are Monteilh v FBI and the City of Irvine SACV 10-00102 JVS (RNBx) and Fazaga v FBI SACV11-00301 CJC (VBKx). I did not create these lawsuits for monetary gain, although it may have appeared to be perceived that way. I gave that appearance purposefully.

The fact is I created these lawsuits so that I may obtain vital and admissible information. Such as court transcripts and documentation only obtained through subpoena power. I desired and sought after this information for two reasons:

1. the FBI reneged on promises made to me that allowed me to be arrested and serve prison time after providing them with vital actionable intelligence and risking my life. I can corroborate this. I orchestrated the lawsuits as my revenge against the FBI. So my purpose was to expose Operation Flex and my participation and also to embarrass the corrupt FBI. And I'm damn proud of it.

2. when Ahmadullah Sais Niazi was arrested February 20, 2009 and the bail hearing that followed my identity was revealed by FBI SA Thomas Ropel III. After the bail hearing the FBI provided me with zero protection and my cover exposed. So as a result I partnered with the ACLU and Council on American Islamic Relations to protect myself from an enraged Islamic community knowing that I worked on behalf of the FBI infiltrating their mosques. The FBI was reckless and negligent.

The information I obtained can only be obtained through declarations, depositions, correspondence between Assistant U.S. Attorney's, Associate General Counsels, email work product, and other discovery documents.

I have had the privilege to interact, communicate and correspond with Associate General Counsels Henry R. Felix, Cecilia O. Bessee, Ted Schwartz, AUSA Thomas K. Buck and FBI attorney Steven Kramer. I have also had the privilege and opportunity to deceive everyone of them. In doing so I now possess a wealth of information that I can now piece together along with the information of my Non-Disclosure Agreement that I signed on October 5, 2007. You may review all of the attached documents.

The wealth of information I obtained by being "The Architect" of *Monteilh v FBI and the City of Irvine* and also *Fazaga v FBI* is as follows:

- Unsealed court documents stating I "provided very, very valuable information that has proved to be essential in an FBI prosecution."
- Acknowledgement by the FBI that I signed a Non-Disclosure Agreement on October 5, 2007.
- Acknowledgement by the FBI that Operation Flex existed and that I was at the center of it.
- Acknowledgement that I worked for the FBI recording information and providing handwritten notes.
- Exposing the FBI agents Kevin Armstrong and Paul Allen as working together with me.
- Linking me to the Ahmadullah Sais Niazi case.
- Revealing that I worked for the FBI until November 2008.
- Revealing SA Paul Allen issuing a national security directive to LA Probation Dept. stating my probation could not be violated due to national security.
- Transcripts revealing SA Paul Allen telling Irvine Police Detective Ron Carr that I was a good asset for the FBI and that I worked well with the FBI.
- Transcripts and recorded information revealing Irvine Police Detective Frough Jahid leaked information to CAIR that I worked for the FBI.

All of the above and even more was revealed because I worked with the ACLU and CAIR. ACLU attorney Peter Bibring and I worked together so that I may get my revenge on the FBI. And it worked. I'll explain my agreement with Mr. Bibring a bit later in my letter. Ahilan Arulanantham was well aware of the agreement with Mr. Bibring.

Please be advised, everything, literally everything that I reveal in this letter the ACLU and the Council on American Islamic Relations have been well aware of. From September 29, 2009 to August 13, 2010 I was represented by them. They kept assuring me that the information I gave them for those 11 months were protected by attorney-client privilege. I am holding them to that privilege.

As a result of the information I obtained the media began to publish all of it (well, 95% of it; you know how lazy they are). I was featured in magazines as *"Mr. Inconspicuous."* Syndicated radio shows as *"The Convert."* Al-Jazeera documentary as *"The Bodybuilder."* News articles as *"Double Agent"* and *"Human Chameleon."* I was even on *Netflix - Hasan Minhaj The Court Jester.* I was published in *The Harvard Law Review.*

Yes, I've done very well for myself considering the FBI tried everything in their power to stop me. I used the same tenacity on Operation Flex as I did on Fazaga v FBI. The main point was always that I'm not a man you fuck with. I don't care if you carry a badge and a gun or even wear a black robe. You fuck with me and I fuck back.

Please understand I forced the FBI to abandon their longstanding policy of neither confirming or denying their sources. Also, I forced them to declassify a classified document in a state secrets case. Two things they never have done before. And I made them do it. I walk and live proud of that.

I am the architect of a lawsuit that has reached the *United States Supreme Court. Case number 20-828.* What an accomplishment. I sleep every night with a smile on my face. Then I wake up with a bigger smile.

Operation Flex:

The narrative that I was a mere FBI confidential human source (CHS) is a blatant lie. To lay a strong foundation before I get into the core of my true role, purpose and the secret results of Operation Flex please understand that confidential human sources **do not** receive FBI issued Joint Terrorism Task Force coins. A CHS **does not** sign classified non-disclosure agreements. A CHS **does not** have a national security operation named in their honor. A CHS **does not** submit to a pre-employment polygraph. A CHS **does not** sit in on classified briefings. A CHS **does not** write daily reports of their operational activity. A CHS **does not** have broad transactional immunity from criminal activity.

All of the above I can corroborate through documentation I have obtained from the 2 lawsuits. I can also corroborate that I was an "FBI employee" for the purpose of the DIOG (FBI's Domestic Investigations and Operations Guide). I was also an employee of the Department of Justice. Please be advised, my designation as an "FBI employee" and Department of Justice employee does not define federal employment for purposes of the Federal Tort Claims Act. It is defined only for the purpose of the DIOG.

To circumvent the DIOG for the sake of national security the FBI through Special Agent Kevin Armstrong personally called the Head Deputy District Attorney Scott Carbaugh in Los Angeles to have my felony probation terminated early so they could justify my employment and justify a proper predicate for the operation. For the purpose of the DIOG I was "operational professional support" and an "FBI contractor."

Former Attorney General Eric Holder asserted privilege over all of the above information while asserting privilege over the most sensitive and classified information, and that information is as follows:

In November and December of 2007 (while still operating under the authority of Operation Flex), FBI SA Kevin Armstrong flew to Pakistan to meet with ISI (Pakistan's Inter-Services Intelligence) with CIA attachment. SA Armstrong had in his possession the whereabouts of Dr. Amin al-Haq, a Specially Designated Global Terrorist. Amin al-Huq was the former security coordinator for Osama bin Laden. The head of the Black Guard.

Amin al-Huq is the brother-in-law of Afghan-born Ahmadullah Sais Niazi of Tustin, CA. During Operation Flex in April of 2007 Mr. Niazi confessed to me (while being recorded) that he was present when Osama bin Laden landed in Afghanistan from Sudan in 1996 along with about 100 mujahideen and Amin al-Huq.

From my recorded conversation with Mr. Niazi the FBI tracked al-Huq's location through Niazi's cell phone communications with his sister and 3 nephews. SA Armstrong oversaw the arrest of Amin al-Huq by ISI and the interrogations that followed. Some enhanced interrogations.

SA Armstrong witnessed the breaking of Amin al-Huq. He gave up the whereabouts of Osama bin Laden in Abbottabad, Pakistan.

He also gave up other names that could corroborate his information. Those individuals were incarcerated at Guantanamo Bay. FBI SA Paul Allen went to Guantanamo Bay in January 2008 to corroborate Amin al-Huq's information. The information was confirmed.

I know all of this because when SA Kevin Armstrong returned from Pakistan he came to the Orange County Jail to visit me along with SA Tracy Hanlon in late December 2007, January 2008, and February 2008. He was also accompanied by FBI attorney Steven Kramer. SA Armstrong visited me approximately 4 times. Those were classified briefings while I was incarcerated.

Former Attorney General Eric Holder asserted privilege over all of the above. Protecting the identity of those CIA assets (SDGT's), and how the assassination of Osama bin Laden actually occurred. **That is the secret**. That is what the government is ultimately protecting. My handwritten notes reveal the April 2007 meeting with Ahmadullah Sais Niazi and the information about his brother-in-law Amin al-Haq.

As time went on, CIA assets confirmed Osama bin Laden was actually at the location in Abbottabad, Pakistan in real time. So finally, on May 1, 2011 President Obama gave the order to kill bin Laden.

As a result, Amin al-Huq and another Specially Designated Global Terrorist by the name of Gulbuddin Hekmatyar became high valued CIA assets. They both are paid assets of the CIA today.

Operation Flex (initially through my intelligence gathering) produced the real time location of Osama bin Laden, resulting in the killing of bin Laden. And I'm damn proud of it. I consider it a duty as an American citizen and am honored to have been the central figure on Operation Flex.

It is shameful how the FBI treated their most valued asset (me). The FBI are scandalous pieces of shit. I would trust a murderous skinhead gang member housed in sol-

itary confinement before I would ever trust an FBI agent. And I have come in close contact with them both.

Operation Flex is one of the most successful FBI operations in the history of the United States. Operation Flex brought justice to the 3,000 Americans killed at the order of the most wanted terrorist in the world.

This concludes Operation Flex and the information the government is protecting through the state secrets privilege.

As for *Fazaga v FBI,* the time has come to end this charade. The declarations that ACLU attorney Peter Bibring and I put together were not necessarily the truth. Mr. Bibring and I came to an agreement that if I signed a contract with the ACLU to cooperate with them then he would have the ACLU write and submit an amicus brief to unseal the court transcripts unveiling my work with the FBI.

After the unsealing I would agree to sign a declaration for the ACLU to be used in a class action lawsuit against the FBI. The contract was agreed upon September 29, 2009. Amicus brief submitted in Citrus Court in West Covina, CA in November 2009. Declaration signed April 23, 2010. And other declarations October 2011. I still possess the ACLU contract.

To be clear, the declarations I signed for the purpose of *Fazaga v FBI* is not accurate information. Most of the information the ACLU (Peter Bibring and Ahilan Arulanantham) and I made up. I do not stand by that information and I will not cooperate with the ACLU to advance 50-60% lies.

Furthermore, I tried to back out of the agreement on August 13, 2010. Peter Bibring and Ahilan Arulanantham refused to return my declaration of April 23, 2010. They stated that I had no right to its return, knowing the information wasn't all accurate. I can verify this through an email communication. Yet they filed it regardless six months later.

I realize the government's petition for rehearing en banc was rejected by the 9th Circuit Court of Appeals and now the government is faced with either petitioning the United States Supreme Court or face remand in the District Court in Santa Ana, CA.

If the government moves to disqualify those declarations I would cooperate and reveal the plan that ACLU attorney Peter Bibring and I agreed to.

This completes my proud creations, and given the opportunity I would do it again and again. Make no mistake, I consider *Fazaga v FBI* a victory for Craig F. Monteilh and his family.

I care about the wasted time of the District Court, the 9th Circuit Court of Appeals and the United States Supreme Court as much as the FBI cared about me and my family.

I am not a victim. And the FBI is no victim. We both willfully did business with one another. Furthermore, the ACLU and the Council on American Islamic Relations used me, and I used them.

Welcome to the gray world of intelligence gathering, deception, manipulation and lies. Let this be a lesson to the almighty, all knowing, arrogant FBI. Every now and then the FBI fucks with the wrong motherfucker. In this case, Craig Monteilh is that motherfucker.

Exhibit A-2

Heiman, Julia (CIV)

From:	Craig Monteilh [**REDACTED**]@yahoo.com>
Sent:	Friday, July 4, 2025 5:58 PM
To:	Ahilan Arulanantham; [**REDACTED**]@aclusocal.org; Trevor Aaronson; Hussain, Suhauna
Cc:	Heiman, Julia (CIV); Hinshelwood, Bradley A. (CIV)
Subject:	[EXTERNAL] Operation Flex/Fazaga v FBI - Volume 2
Attachments:	Op FlexFazagaBlackmail.pdf

Please carefully read the attached.

Exhibit 2

Addition To The Government's Filing Of 6/30/25

The Government's Blackmailing of Craig Monteilh

I, Craig F. Monteilh, have thoroughly reviewed the recent filing of case 8:11-cv-00301-DOC-VBK, Document 192, filed June 30, 2025. Attached in the filing is my 7 page letter I sent from my email to Plaintiffs' and Defendants' attorneys and the press.

While the Government Defendants are currently assessing their next steps in light of my statements, which I knew they would because they are currently in a very desperate position, I must now address a serious matter central to this case that has been ongoing before the inception of this litigation.

The Non-Disclosure Agreement that I signed on October 5, 2007 the FBI/Government attorneys have been using it to blackmail me since my arrest of December 12, 2007.

As I clearly stated in my previous letter, "I'm not a victim," I nevertheless must bring this important matter to the Court's attention. The FBI blackmailing me and my leverage against them is actually accepted forms of behavior in the national security sector. This is not a complaint. These are the facts supported by correspondence between myself and Government attorneys.

FBI Special Agents Kevin Armstrong, Tracy Hanlon, Paul Allen along with FBI attorney Steven Kramer continually reminded me during the timespan of December 12, 2007 to February 2008 not to mention anything about Operation Flex knowing it would exonerate me during my criminal proceedings because I would be violating

my Non-Disclosure Agreement. They said their orders came directly from ASAC Barbara Lee Walls.

I sued the FBI as you know (SACV10-00102) and Judge Selna dismissed the case based on qualified immunity. However, that method of blackmail continued throughout my parole and throughout this entire case. The blackmail has continued for 18 years. They do it because they can and there's no one to stop them. This is an outright abuse of governmental authority. I believe the term used today is: lawfare.

Before I explain how this blackmail has been conducted I must first inform all parties that I brought this matter to ACLU attorney's Peter Bibring, Ahilan Arulanantham, Jenny Pasquarella and Mohammed Tajsar. They were not interested and said I need to retain separate counsel. I instructed them that this blackmail affected the Fazaga case. They didn't care. I personally did not share that information with attorneys for the Council on American Islamic Relations.

According to my recollection, my NDA stated that I, according to law, could not share any information from Operation Flex with anyone outside the signatories. If I did share information about Operation Flex outside of the signatories I would be subjected to imprisonment. That was also explained to me in detail by FBI attorney Steven Kramer and ASAC Barbara Lee Walls.

That is my recollection. Also, I was informed by Mr. Kramer that the NDA is enforceable and would be vigorously enforced if violated.

That said, I tenaciously sought to obtain a copy of my NDA and/or review my NDA knowing what I believed to be very serious consequences if violated.

I contacted the following Associate General Counsels:

- Henry R. Felix - June 15, 2010; July 16, 2010; July 22, 2010; January 5, 2012.
- Cecilia O. Bessee - January 2012
- Julia A. Heiman - emails sent 3/30/25; 4/8/25; 4/9/25; 4/16/25; 4/22/25; 4/25/25.
- Letters to Steven Kramer - January 4 and January 5, 2012.
- Ted Schwartz - July 12, July 26, August 8, August 15, and August 22, 2018.

I possess corroborated documentation of all of the above. I stated my concern of being in jeopardy and risk of losing my freedom.

Associate General Counsel Cecilia O. Bessee outright denied my request for a copy and/or review of my NDA on February 1, 2012. Ms. Bessee stated, "Even if you had complied with the regulations cited above, we would decline your request."

All of this knowing I'm the central focus of a class action lawsuit with national security implications. That is interpreted as leverage. That is outright pressure.

During the course of Monteilh v FBI, Associate General Counsel Henry R. Felix on 3 separate occasions admonished me, "The FBI maintains that all the obligations created under the Non-Disclosure Agreement remain in effect." "Notification by Mr. Monteilh that he intends to disclose information covered by this agreement does not limit or nullify the obligations that he accepted by signing and entering into this agreement."

The above admonishments were dated: June 16, 2010; July 20, 2010; and July 27, 2010.

I also received similar admonishments from Associate General Counsel Ted Schwartz in July and August of 2018.

The main question remains: How in the hell am I to abide by "all the obligations created under the Non-Disclosure Agreement" if the Government attorneys **won't allow me to review** the Non-Disclosure Agreement that I signed? Please read that question again. It makes no sense. It's controlled pressure.

Government attorneys opened the door for me to review and/or receive a copy of my NDA when they declassified a classified document classified at the "Secret" level on 6/25/2015. Case: 13-55017. ID: 9587130.

Government attorneys attached FBI form FD-473 and the signatories were FBI SA Paul Allen and myself on 11/17/06 regarding recording devices on my person while on Operation Flex. If they can attach that then they can surely provide for me to review my NDA.

By denying me any access to my NDA (whether receiving a copy or reviewing it), with the possibility of enforcement, the Government attorneys are holding over my head the threat of imprisonment, fine, and the revoking of thousands of dollars in cash.

And to demonstrate this possibility of enforcement I direct you to the June 8, 2023 hearing before the 9th Circuit Court of Appeals where Government attorney Joseph Busa alluded to that very possibility. Fast forward the hearing to minute 26:30 thru 27:58.

That exchange prompted me to contact Ms. Julia A. Heiman. I assured Ms. Heiman that I only sincerely needed

to review my NDA for the purpose being thoroughly informed so that I would not knowingly place myself in any legal jeopardy.

Ms. Heiman responded that she would get back to me soon and never did. I was clear that I needed to be informed through my NDA so that I would not incriminate myself.

The Government attorneys are indeed blackmailing me. They're using my Non-Disclosure Agreement as leverage. And they absolutely know it. And no one has done shit about it. Having stated the above, I, Craig F. Monteilh, have the right to review and/or possess a copy of my Non-Disclosure Agreement.

Exhibit A-3

Heiman, Julia (CIV)

From:	Craig Monteilh [**REDACTED**]@yahoo.com>
Sent:	Friday, July 11, 2025 10:21 AM
To:	Heiman, Julia (CIV); Hinshelwood, Bradley A. (CIV); Ahilan Arulanantham; [**REDACTED**]@aclusocal.org;
Cc:	Trevor Aaronson; Hussain, Suhauna; [**REDACTED**]@cair.com; Amr Shabaik
Subject:	[EXTERNAL] Clarification and Verification
Attachments:	ClarifyVerify.pdf

Please carefully read the attached.

Exhibit 3

Clarification and Verification

Dear distinguished attorneys for Plaintiffs and Defendants for case No. CV 8:11-cv-00301-DOC-VBK Fazaga v FBI. I, Craig F. Monteilh, have thoroughly reviewed the recent filing of the Joint Status Report filed 7/10/25, Document 193.

There are a few important subjects that I need to clarify and verify. Firstly, I must clarify statements that I made regarding the declarations that ACLU attorneys and I submitted.

The statements are as follows: "The declarations that ACLU attorney Peter Bibring and I put together were not necessarily the truth."

Also, "To be clear, the declarations I signed for the purpose of Fazaga v FBI is not accurate information."

Also, "Most of the information the ACLU (Peter Bibring and Ahilan Arulanantham) and I made up."

And finally, "I do not stand by that information and I will not cooperate with the ACLU to advance 50-60% lies."

All of the above statements I did and knowingly make and I stand by them. However, to be clear, the Government agrees with me. Yes, the Government agrees with me. And this is the clarification:

On August 14, 2012 lead Government attorney Anthony Coppolino stated in Court, "To parse through the truths, half truths and falsehoods" in Monteilh's statements was not possible without wading into sensitive, privileged information.

Mr. Coppolino correctly described my declarations as, "truths, half truths and falsehoods." That description equates and confirms my statement of "50-60% lies." The truths make up for 40-50%. And the half truths and lies make up for the remaining 50-60%.

So there's no argument there. That is my clarification. Furthermore, I would willingly cooperate with a prompt investigation into my contentions. I still possess evidence from Operation Flex. Evidence that ACLU attorneys Peter Bibring and Ahilan Arulanantham willfully overlooked and sought to omit while outlining my declarations. I wanted to add specific information I felt was relevant, however, both ACLU attorneys overruled me, stating it wouldn't look good for the lawsuit.

To be very straightforward regarding my declarations, I personally made every effort to amend them years ago. Specifically the April 23, 2010 declaration. I contacted Defendant's attorneys Alexander Cote, Katie Moran, Howard Shapiro, Catherine Carroll, David Scheper and J. Steinfeld on September 14, 2020 via email. They never returned my message.

The issue with my declarations is nothing new. I contacted Plaintiff's attorneys Peter Bibring, Ahilan Arulanantham, Mohammed Tajsar, Dina Chehata and Amr Shabaik on January 14, 2022; January 18, 2022; January 25, 2022. Peter Bibring reluctantly returned my messages and we began drafts to amend my declaration in late March 2022. Mr. Arulanantham attempted to dissuade me from pursuing any amendments of my declaration stating it wouldn't look good to a judge. I finally approved an amended version late March 2022. The amended version was filed with the Court. I have all of the email communications.

I also read in the Joint Status Report that ACLU attorney Ahilan Arulanantham emphatically denies my statements that ACLU attorneys (including himself) knowingly assisted in the submission of false declarations or engaged in a quid pro quo arrangement for my testimony. That is exactly what they did.

I emphatically challenge his defense and steadfastly stand by my accusations. I have the dates, documentation and email communications as verification. And it all matches. It all verifies.

Attention: Urgent Notice

The Government has given significant credibility to my extraordinary details of Operation Flex specifically with regards to President Obama's order to kill Osama bin Laden.

This is the first time in the 14 year span of the Fazaga v FBI case that the Government raised the issue of protecting the "Executive Branch's Article II powers." Please review Document 193, page 6, in connection to "Mr. Monteilh's allegations."

Secondly, and finally, I must clarify and verify my statement accusing the FBI of reneging on promises made to me that allowed me to be incarcerated.

On or about December 2006 during Operation Flex I signed a classified national security directive giving me the authority and immunity to plan, discuss and conduct terrorist activities with counterterrorism subjects within the continental United States. The signatories were FBI Special Agent Paul Allen, Assistant United States Attorney for the national security section Deirdre Z. Ellioit and myself.

To be clear the directive gave me the authority and immunity to plan, discuss and conduct terrorist activities not execute them. The document I signed was similar to the one I signed on 11/17/06 (FBI FD-473). However, this one was more detailed.

As a paid asset for the FBI I vigorously carried out the directive pretty much on a daily basis. So much so that the Islamic Center of Irvine sought to obtain a restraining order prohibiting me from entering their mosque in June 2007.

A hearing was scheduled for the restraining order. FBI SA Paul Allen instructed me not to defend myself at the hearing. He specifically ordered me not to attend. SA Allen said the order came directly from Assistant Director in Charge J. Stephen Tidwell. The FBI feared that my undercover mission might be compromised during the court proceedings.

SA Allen told me that the restraining order would not have any effect on me and that the FBI would handle the matter. The restraining order was granted and I was prohibited from entering the mosque in Irvine.

On October 5, 2007 I signed a Non-Disclosure Agreement with the FBI with assurances and promises regarding the restraining order, a grand theft case, the termination of probation early, a monetary agreement and an FBI issued Orange County Joint Terrorism Task Force coin.

And then the tragic treacherous nightmare occurred. I was arrested on December 12, 2007 and charged with grand theft.

The FBI as I outlined in my previous letter pressured me to agree to a plea deal with the prosecution. However, I

went to a California State Prison with a terrorist restraining order attached to my file. That terrorist related restraining order enhanced my level of incarceration to a Level IV inmate. Level IV is the most dangerous and serious level in the prison system. I was an inmate housed with the most violent offenders in the state. I was housed with murderers, drug traffickers, kidnappers and validated gang members.

Granted, at the time I was 6'2 275 pounds with the ability to more than adequately defend myself, however, the FBI knowingly and purposefully allowed me to be incarcerated with that terrorism related restraining order in my prison file.

I paroled August 16, 2008 with my parole supervision as **high control**. The status was high control because of the terrorism related restraining order. Parole Division was earnestly looking to violate my parole because they viewed me as a threat to public safety. I have all of the documentation.

There is zero misunderstanding. The Federal Bureau of Investigation conducted themselves in a most treacherous and criminal manner. The FBI has earned my vengeance. Fidelity, Bravery, Integrity. I personally do not doubt the bravery of any law enforcement official. However, fidelity (trust) and integrity (moral values; character; virtue) is a laughable joke when it pertains to the FBI.

This concludes my letter outlining Clarification and Verification.

APPENDIX N

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

No. CV 8:11-cv-00301-DOC-VBK

YASSIR FAZAGA, ET AL., PLAINTIFFS

v.

FEDERAL BUREAU OF INVESTIGATION, ET AL.,
DEFENDANTS

Filed: Sept. 19, 2025

GOVERNMENT DEFENDANTS' NOTICE OF FILING OF ADDITIONAL STATEMENTS OF CRAIG MONTEILH

Defendants the United States of America, Federal Bureau of Investigation, and all Government Defendants sued in their official capacity (collectively "Government Defendants") respectfully submit this notice of filing the additional statements of Mr. Craig Monteilh. After the three emailed statements that the Court admitted into the record as authentic, *see* ECF No. 205, Mr. Monteilh, using the same email address as before, has continued to send statements concerning this litigation to the parties' counsel. The Government Defendants are submitting herewith those additional statements.

Specifically, Mr. Monteilh has sent three such additional statements:

Statement 4: July 15, 2025, Statement[1]

Statement 5: August 19, 2025, Statement

Statement 6: September 9, 2025, Statement

Because the first three of Mr. Monteilh's statements have been admitted into the record as Exhibits 1, 2, and 3, respectively, the Government Defendants continue that numbering in this submission. The Government Defendants have attached a true and correct copy of Mr. Monteilh's fourth, fifth, and sixth statements as Exhibits 4, 5, and 6, respectively.

Also appended hereto as Appendix A is the declaration of undersigned counsel, supplying true and correct copies of Mr. Monteilh's emails transmitting Exhibits 4, 5, and 6.

Dated: September 19, 2025

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General

JEAN LIN
Special Litigation Counsel

---

[1] Out of an abundance of caution, in the fourth statement, the Government Defendants have redacted three names not otherwise associated with this case to protect the privacy of any individuals who may be associated with those names.

/s/ JULIA A. HEIMAN
JULIA A. HEIMAN
Senior Counsel
United States Department
of Justice
Civil Division, Federal Programs
Branch
1100 L Street, NW
Washington, D.C. 20530
Telephone: (202) 616-8480/
Fax: (202) 307-0442
E-mail: julia.heiman@usdoj.gov
Attorneys for the Government
Defendants

Exhibit A-4

Heiman, Julia (CIV)

From:	Craig Monteilh [**REDACTED**]@yahoo.com>
Sent:	Tuesday, July 15, 2025 1:44 PM
To:	Heiman, Julia (CIV); [**REDACTED**]@scheperkim.com
Cc:	[**REDACTED**]@aclusocal.org; Ahilan Arulanantham
Subject:	[EXTERNAL] Context
Attachments:	Context.pdf

Please carefully read the attached.

Exhibit 4

4th Letter From Craig F. Monteilh

Title: Context

Dear Honorable Judge David O. Carter, Defendants attorneys Julia A. Heiman, Alexander Cote and Plaintiffs attorneys Ahilan Arulanantham, Mohammed Tajsar.

Background: The United States, I believe is the greatest country in the world. I truly witnessed something so surreal and astonishing at the July 14, 2025 Status Conference held in Courtroom 10A in Santa Ana, CA at 1:30 pm.

I witnessed in real time the actual Power of the People. As a citizen of the United States of America, I, Craig F. Monteilh, somehow found a way to get into the Court record my three letters without formally taking the witness stand and swearing an oath.

I accomplished this in one of the most important and controversial cases in the country (Fazaga v FBI). A state secrets case. A case that has been dismissed, then appealed before the 9th Circuit Court of Appeals for years, then before the United States Supreme Court, then back to the 9th Circuit, then remanded back to the District Court again and possibly returning to the Supreme Court again.

As the only legally untrained person in the courtroom I managed to dominate the entire hearing with my 3 letters that I sent to Plaintiffs and Defendants attorneys and the press. I was not scheduled to appear or be recognized at that hearing, and yet I and my 3 letters received more time than the actual purpose of that hearing.

That demonstrated to me that government and the judiciary do not rule this country. The People do. I appeared in Court at the Status Conference specifically for the purpose of providing the Court with proper context. I didn't get that opportunity. I was sworn in and Judge Carter only wanted to hear from me either Yes or No if I authored and created the 3 letters. Which is fine. I complied with the Court. So now I'm creating my 4th letter so that I may provide that context knowing now that this 4th letter will also be entered into the Court record.

I will not be so arrogant as to think that I can accomplish this on my own. No, I truly believe a greater power is somehow present.

Relevant Information: The gym and fitness centers are my domain. I have a good reputation in gyms. I socialize in gyms. While I workout I engage in conversations regarding politics, sports, religion, and also that's where I usually engage with women for dating purposes. I workout twice a day.

I also at times use the gyms to conduct my tradecraft. I have gathered actionable intelligence in gyms. I was well known for gathering intelligence in gyms while I worked on the famous national security operation known as Operation Flex which is at issue in this case.

Having stated the above, please now pay attention:

In April of 2013 I met a lovely woman at 24 Fitness in Irvine, CA. Specifically the Jamboree location. This woman is named **[REDACTED]**. Ms. **[REDACTED]** said she was a government employee working out of the FBI office in Orange County.

At that time Ms. **[REDACTED]** was out on disability with a back injury. This was during a time when I began to receive a lot of media attention due to the Fazaga lawsuit, specifically from the public declaration of Assistant Director Mark Giuliano filed August of 2011.

I was featured in a local magazine as "Mr. Inconspicuous." I was also featured in a nationally syndicated radio show as "The Convert." Ms. **[REDACTED]** was highly impressed. She and I spoke at length about my role on Operation Flex.

Ms. **[REDACTED]** and I knew some of the same FBI agents. Ms. **[REDACTED]** and I mutually knew FBI agents from the Criminal Division as well as the Counterterrorism Division.

We discussed plans to date. She provided me with personal information such as that she had an adult son living in Arizona. Ms. **[REDACTED]** ex-husband worked in the FBI's Counterintelligence Division in Los Angeles. Ms. **[REDACTED]** ex-husband infiltrated a Russian KGB cell and was so successful he moved to Moscow for over a year as an undercover agent. I am withholding the name of the FBI Counterintelligence agent for security purposes.

I took copious notes regarding my conversations with Ms. **[REDACTED]**. Ms. **[REDACTED]** compared my role on Operation Flex to her ex-husband's work with the FBI. We bonded in conversations about my spy activities.

One day I brought to the gym my Orange County Joint Terrorism Task Force coin that I received while I worked on Operation Flex. Ms. **[REDACTED]** was astonished that I possessed that coin. Ms. **[REDACTED]** said that those

coins are exclusively set aside for OC-JTTF members and participants. Ms. **[REDACTED]** then viewed me not as an FBI agent but somewhat equal to or better.

At that time Ms. **[REDACTED]** began to pour out information about her knowledge of Operation Flex. Ms. **[REDACTED]** provided me with extensive information about Operation Flex that I already knew which confirmed a lot of information, but also Ms. **[REDACTED]** provided me with an abundance of information about Operation Flex that I did not know.

The abundance of information Ms. **[REDACTED]** provided to me that I did not know is relevant to the Fazaga lawsuit because the information is pertaining to the FBI's surveillance of the Muslim community while I was operational during Operation Flex. Furthermore, the information that I did not know is pertaining to sources and methods, which alarmed me because of my liability from my Non-Disclosure Agreement I signed.

Please be advised, **[REDACTED]** said she is a government employee with a high security clearance with access to FBI classified information.

While out on disability Ms. **[REDACTED]** said she was routinely visited at home by FBI agents checking in on her to protect government secrets. Ms. **[REDACTED]** security clearance covered Chinese intelligence, Russian intelligence and counterterrorism.

During our conversations Ms. **[REDACTED]** said she contacted her coworkers to gain additional information about me and Operation Flex. The co-workers' names are **[REDACTED]** and **[REDACTED]** **[REDACTED]**.

After I received this classified information from Ms. **[REDACTED]** I immediately sought to report it. I con-

tacted ACLU attorney Peter Bibring. I have the emails. I then contacted an Assistant United States Attorney named Thomas K. Buck. I was familiar with AUSA Buck from my personal lawsuit against the FBI. I later contacted Government attorneys informing them. I have those emails also.

AUSA Buck advised me that in all fairness I should inform Ms. **[REDACTED]** that I am involved and am at the center of litigation adverse to the FBI. The advice sounded reasonable. When I informed Ms. **[REDACTED]** she became horrified because of all the information she provided to me. I witnessed the fear in her eyes. At that time she immediately ceased all contact and communication with me.

It is for the above reasons why I sought to amend my declarations. Because of the new relevant information I received from Ms. **[REDACTED]**. The ACLU wouldn't hear of it. They refused. I believe this 4th letter provides the Court with proper context.

Exhibit A-5

Heiman, Julia (CIV)

From:	Craig Monteilh [**REDACTED**]@yahoo.com>
Sent:	Tuesday, August 19, 2025 5:11 PM
To:	Heiman, Julia (CIV); [**REDACTED**]@winston.com; Hussain, Suhauna
Cc:	[**REDACTED**]@latimes.com; Ahilan Arulanantham; [**REDACTED**]@aclusocal.org
Subject:	[EXTERNAL] 5th Letter/Vilify Operation Flex
Attachments:	Villify OP FLEX.pdf

Please carefully read the attached.

Exhibit 5

5th Letter From Craig F. Monteilh

The ACLU of Southern California and Council on American Islamic Relations' agenda to vilify Operation Flex through Fazaga v FBI and USA v Niazi

I, Craig F. Monteilh, the principle and controversial witness in the matter of Fazaga v FBI, case number CV 8:11-cv-00301-DOC-VBK, have thoroughly read the Joint Status Report filed August 14, 2025. I believe I have clearly comprehended the position of Plaintiffs and Government Defendants.

It is my intention in this letter to demonstrate to the Court and the Government the actual strategy and the egregious lengths the ACLU attorneys and attorneys from the Council on American Islamic Relations have gone to advance their agenda with regards to Fazaga v FBI.

First, I will name the attorneys as: Peter Bibring, Ahilan Arulanantham and Amena Qazi. Those three attorneys are the attorneys I interacted with while I was represented by them from the timeframe of September 29, 2009 to August 13, 2010.

I now caution you, the efforts by the ACLU and CAIR **did not** stop at the declarations only. Through the declarations the ACLU and CAIR sought to portray Operation Flex as an illegal and unconstitutional operation that trampled on the civil rights of Muslim Americans. I want to be clear about this, that portrayal is not true. It is the furthest from the truth. And I can corroborate

my assertion through evidence I still possess from Operation Flex.

Secondly, the ACLU and CAIR devised a plan (with my assistance) to control the narrative through the media by portraying Operation Flex as a failed operation that produced no arrests, revealed no terrorist activity and wasted tax payer money while targeting innocent Muslim Americans. Again, that narrative is not true and is the furthest from the truth. I also can corroborate my assertion through the testimony of 2 of the 3 Plaintiffs along with additional evidence I still possess.

Before I get to the most egregious actions of the attorneys I must state for the record what Operation Flex did produce.

- August 2006—only one month into the operation, the apprehension of a bomb maker. There was an Afghan born man who wanted to teach Muslims how to build bombs. The bomb maker solicited his skills during prayer at the Islamic Center of Irvine. That information came to my attention by Yasser Abdel-Rahim and his roommate Ayman Soliman. The information was recorded by me and passed on to the FBI. *** FBI agents were completely astonished at the obvious fact that through my recordings a great many Muslims new this bomb maker existed and openly desired to teach other Muslims to build bombs and not one of them came forward to notify the FBI or any law enforcement ***
- February 2007—uncovering a national security breach. Ahmadullah Sais Niazi worked at the front desk at Berlitz Language Center. The Berlitz Language Center taught foreign languages to virtually every agency in the Intelligence Community. This

includes the CIA, DIA, NSA, FBI, DEA, ATF, military personnel, etc. Mr. Niazi had in his possession the names of thousands of government employees and their affiliated agency. And he actually passed on that information to his associates loyal to Hezb-e-Islami Gulbuddin.

- March 2007—the apprehension of associates of Mustafa Kamal (a Muslim Brotherhood member) and close associate of former FBI informant Osman Umarji.
- March 2007—identifying Mohamed Jaafil as a scout and close associate of Hezbollah. During the 2006 Israel-Hezbollah war, Mohamed Jaafil filmed the entire conflict from his rooftop in Beirut, Lebanon. He played the VHS tape for me while we had lunch in his home. While he was filming he was in touch with Hezbollah fighters guiding them where Israeli solders were located. The United States turned over the tape to the Israeli government. Mohamed Jaafil fled to Lebanon. I recorded the entire luncheon and passed on the recording to the FBI.
- April 2007—My account with Ahmadullah Sais Niazi. Please read the first letter. This was the intelligence that led to the location and killing of Osama bin Laden.

Yes, I was a very busy man during Operation Flex. And as I stated numerous times I'm very proud of my contribution to my country despite the horrific and shameful actions of the FBI towards me. During my time on Operation Flex there were many more apprehensions, thwarted situations and sensitive information acquired.

And now please pay close attention. The ACLU and Council on American Islamic Relations' attorneys explained to me that Operation Flex must appear to be an absolute failure.

Having said that, in October 2008 the FBI obtained a grand jury sealed indictment against Ahmadullah Sais Niazi, case number 8:2009-cr-00028-CJC. Mr. Niazi was arrested February 2009. And that case was dismissed September 2010. There is a reason **why** that case was dismissed. And here is the reason:

On or about March 2010, I received a phone call from ACLU attorney Peter Bibring. Mr. Bibring asked me if I would be willing to meet with Mr. Niazi's attorneys for the purpose of testifying on Mr. Niazi's behalf stating that I willfully entrapped their client. As a result the case would ultimately be dismissed and Operation Flex would appear to be an operation entrapping innocent Muslims.

At the same time Mr. Bibring said that I would be delivering a blow to the FBI. Mr. Bibring said that I couldn't get into any trouble because I was connected to the case and it would be my word against the FBI. A few days later I spoke to Mr. Bibring and Ahilan Arulanantham regarding the Niazi case. I agreed to meet with Mr. Niazi's attorneys. I agreed to do as the ACLU attorneys suggested and planned.

About a week or so later I met with Federal Defenders Chase Scolnick and Guy Iversen. I told them what the ACLU attorneys instructed me to say (that I entrapped Mr. Niazi). And ultimately the case was dismissed and the FBI was humiliated and Operation Flex looked like a failure.

I readily admit my role in obstructing that case. I didn't care. I still don't. The FBI dealt treacherously with me and I dealt treacherously in return. I'm at peace with it. To be very straightforward, every time I think about that case I laugh hysterically. However, that plan was concocted by the ACLU attorneys and as Mr. Bibring and Mr. Arulanantham stated, "its going to make the folks in Anaheim very happy."

I asked, "by Anaheim do you mean CAIR?" They both said, "yes." I've read in the Joint Status Report that the Government quotes me as stating, I "orchestrated the lawsuit as my revenge against the FBI." Let me be clear that I am connected to the words of Shakespeare, *"If you prick us, do we not bleed? If you tickle us, do we not laugh? If you poison us, do we not die? And if you wrong us, shall we not revenge?"—William Shakespeare.*

Exhibit A-6

Heiman, Julia (CIV)

From: Craig Monteilh [**REDACTED**]@yahoo.com>
Sent: Tuesday, September 9, 2025 12:44 PM
To: Heiman, Julia (CIV); [**REDACTED**]@winston.com
Cc: Ahilan Arulanantham; [**REDACTED**]@aclusocal.org; Amr Shabaik; Hussain, Suhauna
Subject: [EXTERNAL] Letter # 6

Attachments: #6 Active Role.pdf

Please carefully read the attached.

Exhibit 6

Letter #6 From Craig F. Monteilh

Dear Honorable David O. Carter, distinguished attorneys for Plaintiffs, and distinguished attorneys for Defendants,

This is my 6th letter. As you have read the previous 5 letters it has become abundantly clear that I have taken an active and vocal role in this lawsuit at this stage. If I may use the quote from the first letter on page 6, "The time has come." And that time is now.

For obvious reasons that you have already previously read, I, and only I, am able to give corroborated testimony to enlighten the Court with accurate information so that the Court may judge what I discern are the remaining core relevant issues that Plaintiffs attorneys and Defendants attorneys are contenting with.

Those core and relevant issues are:

1. The declarations. I am able to demonstrate to the Court with evidence I still possess what information is true and what information is false. Afterwards, Judge Carter will make his ruling.
2. The conduct of ACLU attorneys Peter Bibring and Ahilan Arulanantham, along with Council on American Islamic Relations attorney Ameena Mirza Qazi. I will demonstrate to the Court the evidence I possess and then allow Judge Carter to make his ruling on the conduct of the attorneys.
3. What Plaintiffs attorneys call, "a pattern of unlawful surveillance of Plaintiffs." And concerning "Monteilh's actions over the months he was in the community on the FBI's payroll—where he spent his

> time, who he spent it with, how he behaved as he increasingly tried to draw people into conversation about violence and terrorism."

I am abundantly confident that I am able to intelligently articulate to the Court along with my evidence that the surveillance was indeed lawful and that the above accusations are justified while protecting and preserving the Constitutional rights of Muslim Americans. The FBI's main priority on Operation Flex was to protect and preserve the Constitutional rights of the Muslim community while investigating some members.

And finally, 4. "Plaintiffs' allegations that Defendants targeted the Muslim community for surveillance on the basis of religion."

I am extremely confident that I am able to intelligently articulate to the Court that the surveillance of Operation Flex did not "target" the Muslim community. But rather lawfully followed specific evidence while at the same time protecting the religious rights of the Muslim community.

I am able to provide the Court evidence and testimony to establish a predicate, why I interacted with certain people, and how protections of religious rights were a priority to the FBI for the Muslim community.

It is my hope that this 6th letter provides Honorable David O. Carter and attorneys for both sides some clarity on my intentions to move forward. Thank you.

Side note:

There is something I feel I need to point out. Moreover, its something I want to point out. ACLU attorneys have

no problem pointing out my "extensive criminal history."

While it is true I do have an extensive criminal history, I've been transparent about it and make no apologizes. Yes, I've concentrated on financial crimes and have had success. I possess extraordinary skills. I fooled an entire Muslim community for about 14 months. And I enjoyed it.

However, the ACLU has no problem at all partnering with the Council on American Islamic Relations (aka CAIR) who was designated as an Unindicted Co-conspirator in a terrorism financing case with direct association with Hamas.

USA v Holy Land Foundation for Relief and Development case number CR NO. 3:04-CR-240-G. Page 5, #11 is where you find the designation. It takes a criminal to know a criminal.