FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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. 12-56867 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; J. STEPHEN TIDWELL; BARBARA WALLS,
Defendants,

and

PAT ROSE; KEVIN ARMSTRONG; PAUL ALLEN,
Defendants-Appellants.

No. 12-56874

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

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

Argued and Submitted December 7, 2015
Pasadena, California

Filed February 28, 2019

Before: Ronald M. Gould and Marsha S. Berzon, Circuit Judges and George Caram Steeh III,[*] Senior District Judge.

Opinion by Judge Berzon

SUMMARY[**]

Constitutional Law / Foreign Intelligence Surveillance Act

The panel affirmed in part and reversed in part the district court's judgment in favor of the United States, the FBI, and federal officials in a putative class action alleging that an FBI investigation involved unlawful searches and anti-Muslim discrimination.

Plaintiffs are three Muslim residents of Southern California who alleged that the FBI paid a confidential informant to conduct a covert surveillance program that gathered information about Muslims based solely on their religious identity. Plaintiffs asserted eleven claims, which fell into two categories: claims alleging unconstitutional searches, and claims alleging unlawful religious discrimination. The district court dismissed all but one of plaintiffs' claims on the basis of the state secrets privilege,

[*] The Honorable George Caram Steeh III, Senior District Judge for the U.S. District Court for the Eastern District of Michigan, sitting by designation.

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

and allowed only the Foreign Intelligence Surveillance Act ("FISA") claim against the FBI Agent Defendants to proceed.

The panel held that some of the claims the district court dismissed on state secret grounds should not have been dismissed outright. The panel further held that the district court should have reviewed any state secrets evidence necessary for a determination of whether the alleged surveillance was unlawful following the secrecy-protective procedure set forth in FISA. *See* 50 U.S.C. § 1806(f).

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. Concerning the FISA claim against the Agent Defendants, the panel considered three categories of audio and video surveillance called in the complaint: recordings made by the FBI informant of conversations to which he was a party; recordings made by the informant of conversations to which he was not a party; and recordings made by devices planted by FBI agents. The panel concluded that the Agent Defendants were entitled to qualified immunity as to the first two categories of surveillance. As to the third category of surveillance, the panel held that Agents Allen and Armstrong were not entitled to qualified immunity, but Agents Tidwell, Walls, and Rose were entitled to dismissal as to this category of surveillance because plaintiffs did not plausibly allege their involvement in this category of surveillance.

The panel next addressed the remaining claims, which were all dismissed pursuant to the state secrets privilege. First, the panel held that in determining *sua sponte* that particular claims warranted dismissal under the state secrets privilege, the district court erred. Second, the panel held that

in enacting FISA, Congress displaced the common law dismissal remedy created by the *United States v. Reynolds*, 345 U.S. 1 (1953), state secrets privilege as applied to electronic surveillance within FISA's purview. The panel held that FISA's § 1806(f) procedures were 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. Third, the panel held that the plaintiffs were considered "aggrieved" for purposes of FISA.

The panel next considered whether the claims other than the FISA § 1810 claim must be dismissed for reasons other than the state secrets privilege, limited to reasons raised by the defendants' motions to dismiss.

Addressing plaintiffs' Fourth Amendment search claims, the panel first held that the expungement relief sought by plaintiffs – the expungement of all records unconstitutionally obtained and maintained – was available under the Constitution to remedy the alleged constitutional violations. Because the government raised no other argument for dismissal of the Fourth Amendment injunctive relief claim, it should not have been dismissed. Second, the panel held that in light of the overlap between plaintiffs' *Bivens* claim and the narrow range of the remaining FISA claims against the Agent Defendants that can proceed, it was not clear whether plaintiffs would continue to press this claim. The panel declined to address whether plaintiffs' *Bivens* claim remained available after the Supreme Court's decision in *Ziglar v. Abbasi*, 137 S. Ct. 1843 (2017), and held that on remand the district court may determine whether a *Bivens* remedy is appropriate for any Fourth Amendment claim against the Agent Defendants.

Addressing plaintiffs' claims arising from their allegations that they were targeted for surveillance solely because of their religion, the panel first held that the First Amendment and Fifth Amendment injunctive relief claims against the official-capacity defendants may go forward. Second, concerning plaintiffs' *Bivens* claims seeking 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, the panel concluded that the Privacy Act and the Religious Freedom and Restoration Act ("RFRA"), taken together, provided an alternative remedial scheme for some, but not all, of their *Bivens* claims. As to the remaining *Bivens* claims, the panel remanded to the district court to determine whether a *Bivens* remedy was available in light of the Supreme Court's decision in *Abbasi*. Third, concerning plaintiffs' 42 U.S.C. § 1985(c) claims, alleging that the Agent Defendants conspired to deprive plaintiffs of their First and Fifth Amendment constitutional rights, the panel held that under *Abassi*, intracorporate liability was not clearly established at the time of the events in this case and the Agent Defendants were therefore entitled to qualified immunity from liability under § 1985(c). The panel affirmed the district court's dismissal on this ground. Fourth, concerning plaintiffs' claims that Agent Defendants and Government Defendants violated RFRA by substantially burdening plaintiffs' exercise of religion, and did so without a compelling government interest without the least restrictive means, the panel held that it was not clearly established in 2006 or 2007 that defendants' covert surveillance violated plaintiffs' freedom of religion protected by RFRA. The panel affirmed the district court's dismissal of the RFRA claim as to the Agent Defendants because they were not on notice of a possible RFRA violation. Because the Government

Defendants were 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, the panel held that the complaint stated a RFRA claim against the Government Defendants. Fifth, concerning plaintiffs' allegation that the FBI violated the Privacy Act by collecting and maintaining records describing how plaintiff exercised their First Amendment rights, the panel held that plaintiffs failed to state a claim because the sole requested remedy – injunctive relief – is unavailable for a claimed violation of 5 U.S.C. § 552a(e)(7). Sixth, concerning plaintiffs' claims under the Federal Tort Claims Act ("FTCA"), the panel held that the FTCA judgment bar provision had no application in this case. The panel further held that it could not determine the applicability of the FTCA's discretionary function exception at this stage in the litigation, and that the district court may make a determination of applicability on remand. The panel declined to discuss whether plaintiffs substantively stated claims as to the state laws underlying the FTCA claim.

COUNSEL

Carl J. Nichols (argued) and Howard M. Shapiro, Wilmer Cutler Pickering Hale and Dorr LLP, Washington, D.C.; Katie Moran, Wilmer Cutler Pickering Hale and Dorr LLP, Los Angeles, California; for Defendants-Appellants/Cross-Appellees Barbara Walls and J. Stephen Tidwell.

Alexander H. Cote (argued), Amos A. Lowder, Angela M. Machala, and David C. Scheper, Scheper Kim & Harris LLP, Los Angeles, California, for Defendants-Appellants/Cross-Appellees Pat Rose, Paul Allen, and Kevin Armstrong.

Ahilan Arulanantham (argued), Peter Birbring (argued), and Catherine A. Wagner, ACLU Foundation of Southern California, Los Angeles, California; Ameena Mirza Qazi and Fatima Dadabhoy, Council on American-Islamic Relations, Anaheim, California; Dan Stormer and Mohammad Tajsar, Hadsell Stormer Keeny & Renick LLP, Pasadena, California; for Plaintiffs-Appellees/Cross-Appellants.

Douglas N. Letter (argued), Daniel Tenny, and Mark B. Stern, Appellate Staff; Stephanie Yonekura, Acting United States Attorney; Civil Division, United States Department of Justice, Washington, D.C., for Defendants-Appellees Federal Bureau of Investigation, Christopher A. Wray, and Paul Delacourt.

Richard R. Wiebe, Law Office of Richard R. Wiebe, San Francisco, California; Thomas E. Moore III, Royse Law Firm PC, Palo Alto, California; David Greene, Andrew Crockner, Mark Rumold, James S. Tyre, Kurt Opsahl, Lee Tien, and Cindy Cohn, Electronic Frontier Foundation, San Francisco, California; for Amicus Curiae Electronic Frontier Foundation.

OPINION

BERZON, Circuit Judge:

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.

---

[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 Service Act, 50 U.S.C. § 1810; and the Federal Tort Claims Act, 28 U.S.C. § 1346.

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 determination 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.

[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.

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]

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.

[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."

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

[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)).

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 without 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

[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.

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 privacy* 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

[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).

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 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

[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.

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 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

[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).

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

[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).

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]

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

---

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

"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. 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 *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.

[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.

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 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

[12] We are not suggesting that the recording 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.

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 complaint 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 the Plaintiffs held a subjective expectation of privacy in their conversations among themselves while in the prayer hall.

---

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

---

[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.*

[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)).

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 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

---

[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)).

[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.

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 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

[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).

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 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,

[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 reasonable 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.*

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 requirements 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 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

[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.

[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."

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 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

[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.

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. 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]

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

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 Supreme 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 non-privilege 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 argument 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

[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.

comprehensive legislation or authorized administrative standards," federal 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

[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.

evidentiary privilege absent a clear statement, and that, because Plaintiffs cannot point to a clear statement, "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]

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

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

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 intelligence 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 "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, the Government, in its assertion of the state secrets privilege, has notified the court that it intends to use information obtained or derived from its electronic surveillance of Plaintiffs as part of its defense against Plaintiffs' allegations. *See id.* § 1806(c). Specifically, 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. And the district court's dismissal ruling was premised in part on the potential use of state secrets material to defend the case.

[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.

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 defensive 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)

---

[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).

("[O]ur accusatory system of criminal justice demands that the government seeking 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 initially 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 using a new statute, rule or judicial construction." H.R. Rep. No. 95-1283, pt. 1, at 91 (emphasis added).

---

[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.

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] Some of the Agent Defendants contend that using the § 1806(f) procedures to adjudicate Plaintiffs' claims would violate their due process and Seventh Amendment jury trial rights. This argument is unpersuasive. We and other courts have upheld the constitutionality of the FISA *in*

E. Aggrieved Persons

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

---

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. Mahamud*, 838 F. Supp. 2d 881, 888–89 (D. Minn. 2012); *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.

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 reasons 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] 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

[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 Government 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)).

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 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]

---

[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).

[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.").

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 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. 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

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

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 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

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

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 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

[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.

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 remedial 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

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

§ 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*.

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 Protection 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 assuming 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

[40] Specifically, the plaintiffs alleged that these officials "conspired with one another to hold respondents in harsh conditions because of their actual or apparent race, religion, or national origin." *Abbasi*, 137 S. Ct. at 1854.

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 the 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 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.

---

[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 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).

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]

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

---

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

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 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]

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

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

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 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]

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]

---

[44] These cases do not, however, entitle the Agent Defendants to qualified immunity as to claims involving intentional discrimination based on Plaintiffs' religion. As discussed in *supra* Part IV.B, those claims do not require that Plaintiffs show a substantial burden on the exercise of their religion. That principle was clearly established well before the events in this case. *See, e.g.*, *Lukumi*, 508 U.S. at 546; *Larson v. Valente*, 456 U.S. 228, 244 (1982). Thus, to the extent that Plaintiffs' religion-based *Bivens* claims may proceed, the Agent Defendants are not entitled to qualified immunity for those claims.

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

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 expressly 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

[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)."

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, 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.

---

[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.

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 "materials 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

[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).

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 surveillance, at least for the most

[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).

part, and in nearly all instances entirely,[50] 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 both parties' factual submissions and legal contentions regarding the background of the surveillance. *Id.* (emphasis added).

As we concluded in Part I, *supra*, 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). Only the surveillance in the mosque prayer hall and of Fazaga's office and AbdelRahim's house fits within FISA's definition. But 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, we see no reason why the district court could not then rely on its assessment of the 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.

---

[50] 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 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.

The same categories of evidence will be required to defend against Plaintiffs' surviving claims no matter the particular surveillance at issue. That is, whether the official-capacity defendants targeted Plaintiffs for surveillance in violation of the First Amendment, for example, 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 surveillance in the mosque prayer hall or conversations to which Monteilh was a party. It would be an exercise in empty formalism to require the district court to consider the state secrets evidence *in camera* and *ex parte* to determine the lawfulness of the FISA surveillance, but then ignore that same evidence and so dismiss Plaintiffs' surviving claims as to the non-FISA surveillance. As we explained in our discussion of why FISA's § 1806(f) procedures may be used both for claims arising under § 1810 and under other constitutional and statutory provisions, *see supra* Part II.D, 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 well beyond its purpose to require the district court to consider the state secrets evidence *in camera* and *ex parte* for one purpose, but then ignore it and dismiss closely related claims involving the exact same set of parties, facts, and alleged legal violations.[51]

[51] None of Plaintiffs' legal claims is pleaded to apply only to a particular subset of surveillance activity.

Should our prediction of the close 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,[52] the Government is free to interpose a specifically tailored, properly raised state secrets privilege defense. 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

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

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 entirety, 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.