

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION**

**YASSIR FAZAGA, ALI UDDIN
MALIK, YASSER ABDELRAHIM,**

Plaintiffs,

vs.

**FEDERAL BUREAU OF
INVESTIGATION, ET AL.,**

Defendants.

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

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

I. INTRODUCTION

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

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

18
19 The Attorney General’s privilege claim in this action requires the Court to wrestle
20 with the difficult balance that the state secrets doctrine strikes between the fundamental
21 principles of liberty, including judicial transparency, and national security. Although, as
22 the Ninth Circuit aptly opined, “as judges we strive to honor *all* of these principles, there
23 are times when exceptional circumstances create an irreconcilable conflict between
24 them.” *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1073 (9th Cir. 2010), *cert.*
25 *denied*, 131 S. Ct. 2442 (2011). “On those rare occasions, we are bound to follow the
26 Supreme Court’s admonition that ‘even the most compelling necessity cannot overcome
27 the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake.’ ”
28 *Id.* (quoting *United States v. Reynolds*, 345 U.S. 1, 11 (1953)). Such is the case here.

1 After careful deliberation and skeptical scrutiny of the public and classified filings, the
2 Court concludes that Plaintiffs' claims against Defendants, aside from their FISA claim,
3 must be dismissed under the state secrets privilege.¹ Further litigation of those claims
4 would require or unjustifiably risk disclosure of secret and classified information
5 regarding the nature and scope of the FBI's counterterrorism investigations, the specific
6 individuals under investigation and their associates, and the tactics and sources of
7 information used in combating possible terrorist attacks on the United States and its
8 allies. The state secrets privilege is specifically designed to protect against disclosure of
9 such information that is so vital to our country's national security.

11 **II. BACKGROUND**

12
13 The central subject matter of this case is a group of counterterrorism investigations
14 by the FBI, known as "Operation Flex," which focused on fewer than 25 individuals and
15 "was directed at detecting and preventing possible terrorist attacks." (Pub. Giuliano
16 Decl. ¶ 11.) During the investigations, the FBI utilized Craig Monteilh as a confidential
17 informant from 2006 to 2007. (*Id.* ¶¶ 6, 11.) "The goal of Operation Flex was to
18 determine whether particular individuals were involved in the recruitment and training of
19 individuals in the United States or overseas for possible terrorist activity." (*Id.* ¶ 11.)
20 Plaintiffs allege that as part of Operation Flex, Defendants directed Monteilh to infiltrate
21 mosques and indiscriminately collect information about Plaintiffs and other members of
22 the Los Angeles and Orange County Muslim community because of their adherence to

23
24
25 ¹ Defendants' motions to dismiss Plaintiffs' FISA claim are discussed in the Court's separate,
26 concurrently-issued Order. The Court finds that dismissal of Plaintiffs' FISA claim against the
27 Government is warranted because sovereign immunity has not been waived. The Court, however, finds
28 that Plaintiffs have alleged sufficient facts to state a FISA claim against the individual-capacity Agent
Defendants, who are not entitled to qualified immunity at this stage of the proceeding based on the
allegations pled in the First Amended Complaint.

1 and practice of the religion of Islam from July 2006 to October 2007. (First Amended
2 Complaint (“FAC”) ¶¶ 1–3, 86, 167.)

3
4 The FBI has only acknowledged that Monteilh engaged in confidential source
5 work and disclosed limited information concerning Monteilh’s actions. (Pub. Giuliano
6 Decl. ¶ 6.) For example, in an unrelated criminal proceeding in this district, *United*
7 *States v. Niazi*, Case No. 8:09-cr-28-CJC(ANx), the FBI disclosed to the defendant
8 Ahmadullah Niazi the content of the audio and video recordings containing conversations
9 between him and Monteilh and others. (*Id.* ¶ 12.) The FBI also acknowledged in the
10 *Niazi* case that Monteilh provided handwritten notes to the FBI and that it produced
11 certain notes provided by Monteilh concerning Niazi. (*Id.*)² However, essential details
12 regarding Operation Flex and Monteilh’s activities have not been disclosed, and the
13 Government asserts that this information “remains highly sensitive information
14 concerning counterterrorism matters that if disclosed reasonably could be expected to
15 cause significant harm to national security.” (*Id.* ¶ 6.) The allegedly privileged
16 information includes (i) the identities of the specific individuals who have or have not
17 been the subject of counterterrorism investigations, (ii) the reasons why individuals were
18 subject to investigation, including in Operation Flex, and their status and results, and (iii)
19 the particular sources and methods used in obtaining information for counterterrorism
20 investigations, including in Operation Flex. (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 6.)
21 The Government provides a more fulsome discussion of the nondisclosed matters in its *ex*
22 *parte, in camera* materials that include two classified declarations and a classified
23 supplemental memorandum. (Dkt. Nos. 35, 36, 56.)

24
25
26
27 ² With regard to these materials obtained by Monteilh, the FBI states that is it “presently assessing
28 whether additional audio, video, or notes can be disclosed without risking disclosure of the privileged
information . . . and [risking] significant harm to national security interests in protecting
counterterrorism investigations.” (Pub. Giuliano Decl. ¶ 12.)

1 **A. The Parties**

2
3 Plaintiffs, Sheikh Yassir Fazaga, Ali Uddin Malik, and Yasser AbdelRahim
4 (collectively, “Plaintiffs”), are resident members of the Muslim community in Southern
5 California. (FAC ¶¶ 12–14.) Fazaga, a U.S. citizen born in Eritrea, has served as an
6 “imam” or religious leader of the Orange County Islamic Foundation (“OCIF”), a
7 mosque in Mission Viejo, California, and has lectured widely on topics of Islam and
8 American Muslims. (*Id.* ¶¶ 12, 55–56.) Malik, a U.S. citizen born in Southern
9 California, is a resident of Orange County and has regularly attended religious services at
10 the Islamic Center of Irvine (“ICOI”), a mosque in Irvine, California. (*Id.* ¶¶ 13, 68–69.)
11 AbdelRahim, a U.S. permanent resident from Egypt, has regularly attended religious
12 services at the ICOI. (*Id.* ¶¶ 14, 80.)

13
14 The Government Defendants consist of the FBI and the United States of America
15 as well as Robert Mueller, Director of the FBI, and Steven M. Martinez, Assistant
16 Director in Charge of the FBI Los Angeles Field Office, sued in their official capacities.
17 (*Id.* ¶¶ 15–17, 255.) Defendants also include five FBI agents, Kevin Armstrong, Paul
18 Allen, J. Stephen Tidwell, Barbara Walls, and Pat Rose (collectively, “Agent
19 Defendants”), who are sued in their individual capacities. (*Id.* ¶¶ 18–22.) Defendants
20 Armstrong and Allen, who were both assigned to the Orange County area, were handlers
21 for Monteilh and allegedly directed Monteilh to gather information on the Muslim
22 community in Orange County and also supervised his purported surveillance activities.
23 (*Id.* ¶¶ 18–19, 87.) Defendant Rose, who was assigned to the FBI’s Santa Ana branch
24 office, supervised the FBI’s Orange County national security investigations and directly
25 supervised Allen and Armstrong. (*Id.* ¶ 22.) Defendant Walls, the head of the FBI’s
26 Santa Ana branch office, directly supervised Allen, Armstrong, and Rose. (*Id.* ¶ 21.)
27 Defendant Tidwell served as the Assistant Director in Charge of the FBI’s Los Angeles
28 Field Office from August 2005 to December 2007, and in that capacity, supervised

1 operations in the Central District of California. (*Id.* ¶ 20.) Plaintiffs allege Tidwell
2 authorized the selection of Monteilh as an informant and directed the actions of
3 Armstrong, Allen, Rose, Walls, and other agents in the handling of Monteilh. (*Id.*)
4

5 **B. Operation Flex³**

6

7 Plaintiffs allege many disturbing facts about Operation Flex and wrongdoing by
8 Defendants. Sometime prior to July 2006, Plaintiffs allege that the FBI hired Monteilh to
9 be a paid informant to covertly gather information about Muslims in the Irvine area.
10 (FAC ¶ 48.) Monteilh became a Muslim convert, began to attend the ICOI and five of
11 the other largest mosques in Orange County, and assumed the name Farouk al-Aziz. (*Id.*
12 ¶¶ 49–50, 92.) Monteilh interacted with many members of the Muslim community in
13 Southern California during the relevant time period, including Plaintiffs, as part of a
14 “broader pattern of dragnet surveillance program that Monteilh engaged in at the behest
15 of his FBI handlers,” known as “Operation Flex,” which referenced Monteilh’s cover as a
16 fitness instructor. (*Id.* ¶¶ 54–85, 86, 88.) Armstrong and Allen, who supervised all of
17 Monteilh’s work, informed Monteilh that Operation Flex was part of a broader
18 surveillance program that went beyond his work. (*Id.* ¶ 88.) Defendants did not limit
19 Monteilh to specific targets on which they wanted information, but “repeatedly made
20 clear that they were interested simply in Muslims” and that he should gather “as much
21 information on as many people in the Muslim community as possible,” with heightened
22 attention to particularly religious members and those who attracted Muslim youths. (*Id.*
23 ¶¶ 89, 90, 98.) Plaintiffs allege that “[t]he central feature of the FBI agents’ instructions
24 to Monteilh was their directive that he gather information on Muslims, without any
25 further specification,” and indiscriminately gather information about them under the
26

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

1 maximum that “everybody knows somebody” who may have some connection with the
2 Taliban, Hezbollah, and Hamas. (*Id.* ¶¶ 89, 117.)

3
4 Over the course of Operation Flex, Plaintiffs allege that Armstrong and Allen sent
5 Monteilh to conduct surveillance and audio recording in approximately ten mosques in
6 Los Angeles and Orange County. (*Id.* ¶ 92.) Defendants provided Monteilh with
7 surveillance tools, including sophisticated audio and video recording devices, such as key
8 fobs with audio recording capability and a hidden camera outfitted to his shirt, to conduct
9 an “indiscriminate surveillance” of Muslims, who were targeted “solely due to their
10 religion.” (*Id.* ¶¶ 86, 122, 124, 128.) Defendants gathered information about Plaintiffs
11 and other members of the Muslim community through these devices and from extensive
12 review of Monteilh’s handwritten notes about all aspects of his daily interactions with
13 Muslims. (*Id.* ¶ 122.) Plaintiffs allege that Armstrong and Allen were well aware that
14 many of the surveillance tools they had given Monteilh were being used illegally without
15 warrants. (*Id.* ¶ 136.)

16
17 Plaintiffs allege that the FBI Agents instructed Monteilh to utilize surveillance
18 strategies aimed at gathering information on Muslims in an indiscriminate manner. (*Id.* ¶
19 99.) The Agents’ key directive was that Monteilh gather information from “anyone from
20 any mosque without any specific target, for the purpose of collecting as much
21 information as possible about Muslims in the community.” (*Id.* ¶ 114.) Armstrong and
22 Allen instructed Monteilh to obtain information through various methods, including
23 seizing every opportunity to meet people, obtain their contact information, and learn
24 about their background and religious and political views. (*Id.* ¶ 101.) Monteilh did not
25 limit surveillance to any particular group of people but instead socialized widely with
26 different groups and individuals regardless of their ethnic origin or language. (*Id.* ¶¶
27 102–103.) Armstrong and Allen further instructed Monteilh to gather information on
28 Muslims’ charitable givings, attend Muslim fundraising events, collect information on

1 travel plans of Muslims in the community, attend lectures by Muslim scholars and other
2 guest speakers, attend classes and dawn prayers at mosques, track followers of extremist
3 jihadist websites, elicit people’s views on extremist scholars and thinkers, work out with
4 Muslims he met at a local gym, and gather any compromising information about Muslims
5 that Defendants could use against them to persuade them to become informants. (*Id.* ¶¶
6 105–16.) Plaintiffs allege that the consistent theme throughout these different
7 surveillance gathering strategies was in Armstrong’s and Allen’s “expressed interest in
8 gathering information only on Muslims,” and their setting aside any non-Muslims who
9 were identified through surveillance Monteilh performed. (*Id.* ¶ 120.)

10
11 Plaintiffs allege that through Monteilh, Defendants gathered information on
12 Muslims and their associates consisting of hundreds of phone numbers and thousands of
13 email addresses; background information on hundreds of individuals; hundreds of hours
14 of video recordings that captured the interiors of mosques, homes, businesses, and the
15 associations of Muslims; and thousands of hours of audio recordings of conversations as
16 well as recordings of religious lectures, discussion groups, classes, and other Muslim
17 religious and cultural events occurring in mosques. (*Id.* ¶¶ 2, 137.) Plaintiffs allege that
18 the FBI’s “dragnet investigation did not result in even a single conviction related to
19 counterterrorism” because, unsurprisingly, “the FBI did not gather the information based
20 on suspicion of criminal activity, but instead gathered the information simply because the
21 targets were Muslim.” (*Id.* ¶ 3.) Plaintiffs allege Monteilh discontinued working for
22 Defendants as an informant around September 2007. (*Id.* ¶ 151.)

23
24
25
26 ///

27 ///

28

1 **C. Disclosure of Monteilh’s Identity**

2
3 In February 2009, the FBI acknowledged that it had utilized Monteilh as a
4 confidential informant during a criminal proceeding in the *Niazi* case. (Pub. Giuliano
5 Decl. ¶ 11; FAC ¶¶ 155–59.)⁴ Subsequent to this disclosure, Monteilh has provided
6 numerous statements to the media discussing his purported activities on behalf of the
7 FBI. (Pub. Giuliano Decl. ¶ 14; FAC ¶ 162.)⁵ In January 2010, Monteilh also filed a
8 civil lawsuit under 42 U.S.C. §§ 1983 and 1985 in this district against the FBI, its agents,
9 and the City of Irvine in *Monteilh v. FBI*, Case No. 8:10-cv-102-JVS(RNBx). In that
10 case, Monteilh made allegations related to his work as an FBI source in Operation Flex.
11 (Pub. Giuliano Decl. ¶ 14; FAC ¶ 164.) The FBI has neither confirmed nor denied any of
12 Monteilh’s public allegations concerning his work for the agency, and the FBI maintains
13 that Monteilh’s allegations do not constitute a disclosure or confirmation by the FBI of
14 any information concerning his activities as an informant. (Pub. Giuliano Decl. ¶ 14;
15 FAC ¶ 164.) In this case, Monteilh has submitted a declaration, dated April 23, 2010, in
16 support of Plaintiffs’ opposition to Defendants’ motions to dismiss in which he makes
17 allegations regarding his work for the FBI in Operation Flex similar to those asserted in
18 the FAC. (Dkt. No. 66; FAC ¶ 167.)

19
20 **D. The Lawsuit**

21
22 On February 22, 2011, Plaintiffs filed the instant suit against the FBI and its
23 officers and agents. (Dkt. No. 1.) On August 1, 2011, the FBI, Mueller, and Martinez
24 moved to dismiss the Complaint and for summary judgment on the grounds, *inter alia*,

25
26 _____
27 ⁴ This Court dismissed the *Niazi* indictment without prejudice on September 30, 2010. (Case No. 8:09-
28 cr-28-CJC(ANx), Ct. Order, Dkt. No. 40, Sept. 30, 2010.)

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

1 that certain evidence needed to litigate Plaintiffs' claims is properly protected by the
2 Attorney General's assertion of the state secrets privilege. (Dkt. No. 32.) In support of
3 their privilege claim, they submitted for *ex parte, in camera* review by the Court (i) a
4 classified declaration of Mark F. Giuliano, FBI Assistant Director, Counterterrorism
5 Division and (ii) a classified supplemental memorandum. (Dkt. Nos. 35, 36.) The Agent
6 Defendants also separately moved to dismiss the Complaint. (Dkt. Nos. 41–42.) Shortly
7 thereafter, Plaintiffs moved *ex parte* to stay the Court's review of the classified filings
8 until after its consideration of whether the state secrets argument would apply in this case
9 as a matter of law. (Dkt. No. 39.) Plaintiffs argued that such a ruling would prevent the
10 Court from unnecessarily reviewing information that could be highly prejudicial to
11 Plaintiffs and not properly subject to consideration by the Court. (Pls. Ex Parte App., at
12 8.) The Court denied Plaintiffs' *ex parte* application because the Court determined that
13 there was no legal bar to its review of the classified submissions and because it was
14 confident that its independent evaluation would not be compromised by the contents of
15 those submissions. (Ct. Order, Dkt. No. 46, Aug. 11, 2011.)

16
17 On September 13, 2011, Plaintiffs filed the operative FAC, adding a claim under
18 the FTCA against the United States. (Dkt. No. 49.) Plaintiffs assert a total of eleven
19 causes of action against Defendants: (1) violation of the First Amendment Establishment
20 Clause under *Bivens* and 28 U.S.C. § 1331 (against all Defendants except the FBI and
21 United States); (2) violation of the First Amendment Establishment Clause under 42
22 U.S.C. § 1985(3) and 28 U.S.C. § 1343 (against Agent Defendants); (3) violation of the
23 First Amendment Free Exercise Clause under *Bivens* and 28 U.S.C. § 1331 (against all
24 Defendants except the FBI and United States); (4) violation of the First Amendment Free
25 Exercise Clause under 42 U.S.C. § 1985(3) and 28 U.S.C. § 1343 (against Agent
26 Defendants); (5) violation of RFRA, 42 U.S.C. § 2000bb-1 (against all Defendants);
27 (6) violation of the Fifth Amendment Equal Protection Clause under *Bivens* and 28
28 U.S.C. § 1331 (against all Defendants except the FBI and United States); (7) violation of

1 the Equal Protection Clause under 42 U.S.C. § 1985(3) and 28 U.S.C. § 1343 (against
2 Agent Defendants); (8) violation of the Privacy Act, 5 U.S.C. § 552a(a)–(l) (against the
3 FBI); (9) violation of the Fourth Amendment under *Bivens* and 28 U.S.C. § 1331 (against
4 the FBI and United States); (10) violation of FISA, 50 U.S.C. § 1810 (against all
5 Defendants); and (11) invasion of privacy, violation of Cal. Civ. Code § 52.1, and
6 intentional infliction of emotion distress under the FTCA, 28 U.S.C. §§ 1346(b), 2671, *et*
7 *seq.* (against the United States).⁶ Plaintiffs request damages as well as injunctive relief in
8 the form of the destruction or return of any information gathered through Operation Flex.
9 Plaintiffs further seek certification of “[a]ll individuals targeted by Defendants for
10 surveillance or information-gathering through Monteilh and Operation Flex, on account
11 of their religion, and about whom the FBI thereby gathered personally identifiable
12 information.” (FAC ¶ 219.)

13
14 On November 4, 2011, the Government moved to dismiss the FAC and for
15 summary judgment pursuant to Federal Rules of Civil Procedure 12(b)(1), 12(b)(6), and
16 56. (Dkt. No. 55.) The Government moves to dismiss all of Plaintiffs’ claims, aside
17 from the FISA and Fourth Amendment claims, on the grounds that, *inter alia*, litigation
18 of these claims would risk or require the disclosure of certain evidence properly protected
19 by the Attorney General’s assertion of the state secrets privilege. In support of their
20 privilege claim, the Government relies on its previously-filed public declaration from the
21 Attorney General, Eric H. Holder, dated July 29, 2011, (Dkt. No. 32-3), and a public
22 declaration from Mark Giuliano, dated July 25, 2011, (Dkt. No. 33). The Government
23 also relies on its previously-lodged, August 1, 2011 *in camera* filings, the classified
24 declaration of Giuliano and the classified supplemental memorandum, (Dkt. Nos. 35, 36).
25 In addition, the Government lodged a classified supplemental declaration of Giuliano on
26

27
28 ⁶ For claims 1, 3, 6, and 9, Plaintiffs assert claims for damages under *Bivens* against individual-capacity Agent Defendants and assert claims for injunctive relief under Section 1331 against the official-capacity Defendants. (*See* FAC ¶ 226 n.37.)

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

3
4 Defendants Tidwell and Walls separately moved to dismiss claims against them
5 under Federal Rule of Civil Procedure 12(b)(6). (Dkt. No. 58.) Tidwell and Walls argue,
6 in part, that the Government’s assertion of the state secrets privilege mandates dismissal
7 of Counts 1 through 7. (Tidwell/Walls Br., at 9–12.) Defendants Rose, Armstrong, and
8 Allen also moved to dismiss the FAC under Rule 12(b)(6) and joined in the motions to
9 dismiss filed by the Government and Defendants Tidwell and Walls. (Dkt. No. 57.) On
10 December 23, 2011, Plaintiffs opposed the Government’s motion and filed a combined
11 opposition to the Agent Defendants’ motions to dismiss. (Dkt. Nos. 63, 64.) Defendants
12 filed replies in support of their respective motions to dismiss on January 20, 2012. (Dkt.
13 Nos. 69–71.) After granting the parties’ requests for continuances of the hearing on
14 Defendants’ motions to dismiss, the Court heard extended oral arguments on the motions
15 from the parties’ counsel on August 14, 2012.

16 17 **III. LEGAL STANDARD**

18 19 **A. The State Secrets Doctrine**

20
21 “The Supreme Court has long recognized that in exceptional circumstances courts
22 must act in the interest of the country’s national security to prevent disclosure of state
23 secrets, even to the point of dismissing a case entirely.” *Jeppesen Dataplan*, 614 F.3d at
24 1077 (citing *Totten v. United States*, 92 U.S. 105, 107 (1875)). Created by federal
25 common law, the state secrets doctrine bars litigation of an action entirely or excludes
26 certain evidence because the case or evidence risks disclosure of “state secrets”—that is,
27 “matters which, in the interest of national security, should not be divulged.” *Reynolds*,
28 345 U.S. at 10. Although developed at common law, the state secrets doctrine also

1 “performs a function of constitutional significance, because it allows the executive
2 branch to protect information whose secrecy is necessary to its military and foreign-
3 affairs responsibilities.” *El-Masri v. United States*, 479 F.3d 296, 303 (4th Cir. 2007). At
4 the same time, the state secrets doctrine does not represent an abdication of judicial
5 control over access to the courts, as the judiciary is ultimately tasked with deciding
6 whether the doctrine properly applies to a particular case. *Id.* at 312. The state secrets
7 doctrine thus attempts to strike a difficult balance between the Executive’s duty to protect
8 national security information and the judiciary’s obligation to preserve judicial
9 transparency in its search for the truth. *Id.* at 303–305.

10
11 There are two modern applications of the state secrets doctrine: (1) a justiciability
12 bar that forecloses litigation altogether because the very subject matter of the case is a
13 state secret (the “*Totten* bar”) and (2) an evidentiary privilege that excludes certain
14 evidence because it implicates secret information and may result in dismissal of claims
15 (the “*Reynolds* privilege”). *Jeppesen Dataplan*, 614 F.3d at 1077–80. While distinct, the
16 *Totten* bar and the *Reynolds* privilege converge in situations where the government
17 invokes the privilege—as it may properly do—before waiting for an evidentiary dispute
18 to arise during discovery or trial. *Id.* at 1080 (“The privilege may be asserted at any time,
19 even at the pleading stage.”). The privilege indisputably may be raised with respect to
20 discovery requests seeking allegedly privileged information or to prevent disclosure of
21 such information in a responsive pleading. *Id.* at 1081. Alternatively, “the government
22 may assert a *Reynolds* privilege claim prospectively, even at the pleading stage, rather
23 than waiting for an evidentiary dispute to arise during discovery or trial.” *Id.* In such
24 circumstances, the *Totten* bar necessarily informs the *Reynolds* privilege in a “continuum
25 of analysis.” *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1201 (9th Cir.
26 2007).

1 **1. The Totten Bar**

2
3 The Supreme Court in *Totten v. United States* articulated the general principle that
4 “public policy forbids the maintenance of any suit in a court of justice, the trial of which
5 would inevitably lead to the disclosure of matters which the law itself regards as
6 confidential.” 92 U.S. at 107. The *Totten* bar is a categorical bar “where the very subject
7 matter of the action . . . [is] a matter of state secret,” such that the action is “dismissed on
8 the pleadings without ever reaching the question of evidence since it [is] so obvious that
9 the action should never prevail over the privilege.” *Reynolds*, 345 U.S. at 11 n.26;
10 accord *Jeppesen Dataplan*, 614 F.3d at 1077–78; see also *Al-Haramain*, 507 F.3d at
11 1197 (“[W]here the very subject matter of a lawsuit is a matter of state secret, the action
12 must be dismissed without reaching the question of evidence.”). The purpose of the
13 *Totten* bar is not merely to defeat the asserted claims, but to foreclose judicial inquiry
14 altogether. *Tenet v. Doe*, 544 U.S. 1, 6 n.4 (2005); *Jeppesen Dataplan*, 614 F.3d at 1078.

15
16 The Supreme Court has very sparingly applied this bar to preclude judicial review
17 of an action entirely. See *Totten*, 92 U.S. at 106–107 (barring suit by Civil War spy
18 against the United States for alleged failure to pay for espionage services because the
19 case was predicated on the existence of an undisclosed contract for secret services with
20 the government); *Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454
21 U.S. 139, 146–47 (1981) (holding action against the United States Navy exceeded
22 judicial scrutiny based on state secrets because it implicated information regarding
23 nuclear weapons storage that the Navy could not admit or deny); *Tenet*, 544 U.S. at 8–10
24 (precluding judicial review of action by former Cold War spies against the Central
25 Intelligence Agency for allegedly reneging on promise to pay for espionage services
26 because plaintiffs’ relationship with the government was state secrets). Beyond these
27 three cases, the Supreme Court has not provided further guidance on what subject matters
28 would constitute state secrets. The Ninth Circuit in *Jeppesen*, however, declined to

1 interpret the *Totten* bar as only applying to certain types of cases, such as those involving
2 covert espionage agreements, but emphasized that “the *Totten* bar rests on a general
3 principle that extends beyond that specific context” and applies “‘where the very subject
4 matter of the action’ is ‘a matter of state secret.’” 614 F.3d at 1078–79 (quoting
5 *Reynolds*, 345 U.S. at 11 n.26). The *El-Masri* court further clarified that “[t]he
6 controlling inquiry is not whether the general subject matter of an action can be described
7 without resort to state secrets”; rather, it must be ascertained “whether an action can be
8 *litigated* without threatening the disclosure of such state secrets.” *El-Masri*, 479 F.3d at
9 308. “Thus, for purposes of the state secrets analysis, the ‘central facts’ and ‘very subject
10 matter’ of an action are those facts that are essential to prosecuting the action or
11 defending against it.” *Id.*

12

13 **2. The Reynolds Privilege**

14

15 The second application of the state secrets doctrine is an evidentiary privilege
16 against revealing state secrets. *Jeppesen Dataplan*, 614 F.3d at 1079. Derived from
17 *United States v. Reynolds*, this privilege applies when the court is satisfied “from all the
18 circumstances of the case, that there is a reasonable danger that compulsion of the
19 evidence will expose . . . matters which, in the interest of national security, should not be
20 divulged.” *Reynolds*, 345 U.S. at 10; *see also id.* at 10–11 (finding that the government
21 made a sufficient showing of privilege, “under circumstances indicating a reasonable
22 possibility that military secrets were involved,” to cut off demand for an accident
23 investigation report of an aircraft testing secret electronic equipment). A successful
24 assertion of the *Reynolds* privilege will remove the privileged evidence from the case.
25 *Jeppesen Dataplan*, 614 F.3d at 1079. In some instances, however, “the assertion of the
26 privilege will require dismissal because it will become apparent during the *Reynolds*
27 analysis that the case cannot proceed without privileged evidence, or that litigating the
28 case to a judgment on the merits would present an unacceptable risk of disclosing state

1 secrets.” *Id.* The Ninth Circuit in *Jeppesen Dataplan* applied the *Reynolds* privilege to
2 dismiss an action brought by foreign nationals who were allegedly transported in secret to
3 other countries where they were detained and interrogated under the Central Intelligence
4 Agency’s (“CIA”) extraordinary rendition program. 614 F.3d at 1085–90. The Ninth
5 Circuit held that dismissal under the state secrets privilege was required under *Reynolds*
6 because there was no feasible way to litigate the defendant’s liability without creating “an
7 unjustifiable risk of divulging state secrets” related to the CIA’s secret intelligence
8 activities. *Id.* at 1087. When such dismissal is required, the *Reynolds* privilege
9 converges with the *Totten* bar. *Id.* at 1083.

10
11 An analysis of claims under the *Reynolds* privilege involves three steps. First, the
12 court must ascertain whether the procedural requirements for invoking the privilege,
13 consisting of a formal claim by the government, have been satisfied. *Id.* at 1080.
14 Second, the court must independently determine whether the information is privileged.
15 *Id.* Third, the court must determine how the case should proceed in light of the
16 successful privilege claim. *Id.* Once the privilege is properly invoked, and the court is
17 satisfied as to the danger of disclosing state secrets, the privilege is absolute. *Kasza v.*
18 *Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *see also Reynolds*, 345 U.S. at 11
19 (“[E]ven the most compelling necessity cannot overcome the claim of privilege if the
20 court is ultimately satisfied that [state] secrets are at stake.”); *In re United States*, 872
21 F.2d 472, 476 (D.C. Cir. 1989) (“No competing public or private interest can be
22 advanced to compel disclosure [of privileged information].” (citation and quotes
23 omitted)). This is because, in determining whether the privilege applies to a particular
24 case, “the balance has already been struck in favor of protecting secrets of state over the
25 interest of a particular litigant.” *In re United States*, 872 F.2d at 476 (citation and quotes
26 omitted). The Supreme Court has therefore cautioned that the privilege “is not to be
27 lightly invoked,” and must be applied no more often or extensively than necessary.
28 *Reynolds*, 345 U.S. at 7–8; *see also Jeppesen Dataplan*, 614 F.3d at 1080.

1 **B. Threshold Considerations**

2
3 Plaintiffs raise two threshold issues with regard to whether the state secrets
4 doctrine may apply in this case, neither of which are persuasive. First, Plaintiffs argue
5 that FISA preempts the state secrets privilege. Plaintiffs insist that because most, if not
6 all, of the conduct at issue in this case involves electronic surveillance in the name of
7 foreign intelligence gathering in the domestic context, the Court should adhere to the
8 procedures that Congress has set for the treatment of secret evidence in FISA.⁷ (Pls.
9 Opp’n to Gov’t, at 20–21, 26–31.) The Court disagrees. As a preliminary matter, the
10 question of whether FISA preempts the state secrets privilege is not at issue because
11 Defendants have not moved to dismiss the FISA claim on privilege grounds. Moreover,
12 even if FISA preempts the state secrets privilege with respect to a FISA claim, as ruled
13 by the Northern District of California in *In re Nat’l Sec. Agency Telecomms. Records*
14 *Litig.*, 564 F. Supp. 2d 1109, 1120 (N.D. Cal. 2008),⁸ Plaintiffs cite no authority for the
15 proposition that FISA also preempts non-FISA claims. Nor has the Court found any
16 statute, including the language of FISA, or case law supporting an expansive application
17 of FISA to Plaintiffs’ non-FISA claims in this case. Plaintiffs rely on *In re National*
18 *Security Agency*, 564 F. Supp. 2d at 1118, for the proposition that FISA preempts the
19 state secrets privilege in cases, as here, which involve electronic surveillance undertaken
20 in the name of national security. (Pls. Opp’n to Gov’t, at 26, 29). However, the court in
21 that case clarified that “FISA does not preempt the state secrets privilege as to matters
22 that are not within FISA’s purview,”—that is, “activities [that] include foreign
23 intelligence surveillance.” *In re National Security Agency*, 564 F. Supp. at 1118. In the
24

25 ⁷ See the Court’s concurrently-filed Order, which discusses the FISA claim in detail.

26 ⁸ The Court *In re National Security* determined that “FISA should displace federal common law rules
27 such as the state secrets privilege with regard to matters within FISA’s purview.” 564 F. Supp. 2d at
28 1120. As the Government does not move to dismiss the FISA claim on the basis of state secrets, the
Court need not and does not decide at this time whether FISA preempts the state secrets privilege with
respect to a FISA claim.

1 present action, however, the central subject matter is Operation Flex, a group of
2 counterterrorism investigations that extend well beyond the purview of electronic
3 surveillance as discussed in the Government’s public and classified filings. Plaintiffs’
4 non-FISA claims also rely upon allegations far broader in scope than allegations upon
5 which the FISA claim is predicated, and litigating those non-FISA claims will require
6 information, including privileged evidence, beyond that contemplated by FISA. (*See*
7 *infra* Part IV.C.)

8
9 Second, Plaintiffs argue that the Constitution prohibits dismissal of this case on
10 state secret grounds because they seek injunctive relief from on-going constitutional
11 violations. (Pls. Opp’n to Gov’t, at 20, 40–51.) This argument, likewise, is unsupported
12 by any authority, let alone Ninth Circuit or Supreme Court precedent. The principles of
13 the state secrets doctrine make clear that it is analyzed and applied to cases irrespective of
14 the types of claims or relief sought. *See Tenet*, 544 U.S. at 8 (“[P]ublic policy forbids the
15 maintenance of *any suit* in a court of justice, the trial of which would inevitably lead to
16 the disclosure of matters which the law itself regards as confidential.” (quoting *Totten*, 92
17 U.S. at 107)); *Kasza*, 133 F.3d at 1166 (“Once the privilege is properly invoked and the
18 court is satisfied as to the danger of divulging state secrets, the privilege is absolute. . .
19 .”); *Jeppesen Dataplan*, 614 F.3d at 1081 (“If this standard [for privilege] is met, the
20 evidence is absolutely privileged, irrespective of the plaintiffs’ countervailing need for
21 it.”). In fact, in *Al-Haramain*, the Ninth Circuit found that the state secrets privilege
22 applied to and warranted dismissal of constitutional claims involving requests for
23 injunctive relief. 507 F.3d at 1205. In that case, Al-Haramain Islamic Foundation, a
24 designated terrorist organization, and two of its attorneys brought suit against the
25 government in connection with the government’s Terrorist Surveillance Program. 507
26 F.3d at 1193. The plaintiffs in that case alleged that they were subject to warrantless
27 electronic surveillance in violation of FISA and various provisions of the Constitution.
28 *Id.* In addition to a request to enjoin further warrantless surveillance, the plaintiffs sought

1 the same injunctive relief as Plaintiffs here do—disclosure and/or destruction of
2 information and records acquired from allegedly unlawful surveillance—and also
3 similarly alleged violations under the First and Fourth Amendments. *Al-Haramain*
4 *Islamic Found., Inc. v. Bush*, 451 F. Supp. 2d 1215, 1218 (D. Or. 2006), *rev'd and*
5 *remanded by Al-Haramain*, 507 F.3d 1190. The Ninth Circuit in *Al-Haramain* found
6 dismissal of the action appropriate under the *Reynolds* privilege because the defendant
7 could not establish standing without the privileged information. 507 F.3d at 1205.⁹
8 Accordingly, the Court finds that the state secrets doctrine may properly be considered in
9 this case.

11 **IV. APPLICATION OF THE STATE SECRETS DOCTRINE**

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

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

1 that dismissal of Plaintiffs' claims, aside from their FISA claim, is required under the
2 *Reynolds* privilege.

3 4 **A. Procedural Requirements**

5
6 The *Reynolds* privilege may only be asserted by the government, and a private
7 party can neither claim nor waive the privilege. *Jeppesen Dataplan*, 614 F.3d at 1080;
8 *Reynolds*, 345 U.S. at 7. The government cannot invoke the privilege lightly, especially
9 where it seeks not merely to preclude the production of certain evidence, but to obtain
10 dismissal of the action entirely. *Jeppesen Dataplan*, 614 F.3d at 1080. There are several
11 mechanisms to ensure that the *Reynolds* privilege is invoked no more than is necessary.
12 *Id.* First, “[t]here must be a formal claim of privilege, lodged by the head of the
13 department which has control over the matter, after actual personal consideration by that
14 officer.” *Reynolds*, 345 U.S. at 7–8. “This certification is fundamental to the
15 government’s claim of privilege,” as the decision to invoke the privilege must “‘be a
16 serious, considered judgment, not simply an administrative formality.’” *Jeppesen*
17 *Dataplan*, 614 F.3d at 1080 (quoting *United States v. W.R. Grace*, 526 F.3d 499, 507–508
18 (9th Cir. 2008) (en banc)). The formal claim must “reflect the certifying official’s
19 *personal* judgment,” and be presented in “sufficient detail” to permit the court “to make
20 an independent determination of the validity of the claim of privilege and the scope of the
21 evidence subject to the privilege.” *Id.* at 1080.

22
23 Second, even before invoking the privilege in court, the government must adhere
24 to its own State Secrets Policy, promulgated by the Obama administration in a
25 memorandum by the Attorney General in September 2009, effective October 1, 2009.
26 (Holder Decl. ¶ 12 & Exh. 1 [State Secrets Policy]); *see also Jeppesen Dataplan*, 614
27 F.3d at 1077. The Policy outlines the legal standard for invoking the privilege: the
28 government will assert and defend an assertion of the state secrets privilege in litigation

1 “when a government department or agency seeking to assert the privilege makes a
2 sufficient showing that assertion of the privilege is necessary to protect information the
3 unauthorized disclosure of which reasonably could be expected to cause significant harm
4 to the national defense or foreign relations (“national security”) of the United States.”
5 (Holder Decl., Exh. 1 ¶ 1(A).) The privilege must also be “narrowly tailored,” such that
6 the “privilege should be invoked only to the extent necessary to protect against the risk of
7 significant harm to national security.” (*Id.* ¶ 1(B).) The Policy further sets limitations for
8 invoking the privilege, including not defending an invocation of the privilege to “conceal
9 violations of the law, inefficiency, or administrative error”; to “prevent embarrassment to
10 a person, organization, or agency of the United States government”; or to “prevent or
11 delay the release of information the release of which would not reasonably be expected to
12 cause significant harm to national security. (*Id.* ¶ 1(C).) The Policy further outlines the
13 initial procedure for invoking the privilege, which includes sufficient evidentiary support
14 and recommendation from the Assistant Attorney General; evaluation, consultation, and
15 recommendation by a state secrets review committee; and approval by the Attorney
16 General. (*Id.* ¶¶ 2–4.)

17
18 The Government has properly invoked the state secrets privilege. The Government
19 has submitted a public declaration from Eric Holder in his capacity as the Attorney
20 General and head of the Department of Justice. The Attorney General has made a formal
21 assertion of the state secrets privilege after personal consideration of the public and
22 classified materials at the request of the director of the FBI: “After careful and actual
23 personal consideration of the matter, I have concluded that disclosure of the three
24 categories of information described below and in more detail in the classified Giuliano
25 Declaration could reasonably be expected to cause significant harm to the national
26 security, and I therefore formally assert the state secrets privilege over this information.”
27 (Holder Decl. ¶ 3.) The Attorney General also avers that the requirements for an
28

1 assertion and defense of the state secrets privilege have been satisfied in accordance with
2 the State Secrets Policy. (*Id.* ¶ 12.)¹⁰

3 4 **B. Independent Evaluation of the Privilege Claim**

5
6 After a court determines that the privilege has been properly invoked, it then
7 “‘must make an independent determination whether the information is privileged.’”
8 *Jeppesen Dataplan*, 614 F.3d at 1080, 1081 (quoting *Al-Haramain*, 507 F.3d at 1202).
9 “‘The court must sustain a claim of privilege when it is satisfied, ‘from all the
10 circumstances of the case, that there is a reasonable danger that compulsion of the
11 evidence will expose . . . matters which, in the interest of national security, should not be
12 divulged.’” *Id.* at 1081 (quoting *Reynolds*, 345 U.S. at 10). “‘The Executive bears the
13 burden of satisfying a reviewing court that the *Reynolds* reasonable-danger standard is
14 met.” *El-Masri*, 479 F.3d at 305. The government cannot satisfy this burden by the mere
15 conclusory assertion that the standard has been met. *El-Masri*, 479 F.3d at 312. “‘Simply
16 saying ‘military secret,’ ‘national security’ or ‘terrorist threat’ or invoking an ethereal
17 fear that disclosure will threaten our nation is insufficient to support the privilege.” *Al-*
18 *Haramain*, 507 F.3d at 1203. Rather, the government must provide “[s]ufficient detail” to
19 enable the court to conduct a meaningful examination. *Id.* In some instances, a formal
20 privilege claim asserted in a declaration may suffice, while in others, the court may
21 conduct an *in camera* examination of the allegedly privileged information. *El-Masri*, 479

22
23 ¹⁰ The Court cannot and does not comment on whether the Government has properly adhered to its State
24 Secrets Policy, as this is internal to the Executive branch, and the Policy does not create a substantive or
25 procedural right enforceable at law or in equity against the Government. (*See* Holder Decl., Exh. 1 ¶ 7.)
26 However, the Court does observe that the Government has narrowly tailored its assertion of the privilege
27 by moving on other grounds before invoking the privilege and has done so with restraint. (*See* Gov’t
28 Br., at 3–7.) While the Court has considered Defendants’ initial grounds for dismissal before analyzing
the state secrets privilege, the Court believes they are limited and do not entirely warrant dismissal of
Plaintiffs’ claims. In contrast, the Court finds that all of Plaintiffs’ claims, aside from their FISA claim,
should be dismissed under the *Reynolds* privilege. For this reason and for the sake of judicial economy,
the Court limits its discussion to the state secrets doctrine in this Order and the FISA claim in the
Court’s concurrently-issued Order.

1 F.3d at 305. “The degree to which such a reviewing court should probe depends in part
2 on the importance of the assertedly privileged information to the position of the party
3 seeking it.” *Id.*; *see also Reynolds*, 345 U.S. at 11 (“In each case, the showing of
4 necessity which is made will determine how far the court should probe in satisfying itself
5 that the occasion for invoking the privilege is appropriate.”) At the same time, the Court
6 must make this determination “without forcing a disclosure of the very thing the privilege
7 is designed to protect.” *Reynolds*, 345 U.S. at 8. “If this standard is met, the evidence is
8 absolutely privileged, irrespective of the plaintiffs’ countervailing need for it.” *Jeppesen*
9 *Dataplan*, 614 F.3d at 1081.

10
11 Here, the Government asserts the privilege over three categories of information
12 related to Operation Flex as described in their public and classified filings: (i) subject
13 identification, (ii) reasons for counterterrorism, and (iii) sources and methods. First, the
14 FBI seeks to protect “[i]nformation that could tend to confirm or deny whether a
15 particular individual was or was not the subject of an FBI counterterrorism investigation,
16 including in Operation Flex.” (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 15.) Second, the
17 FBI seeks to protect “[i]nformation that could tend to reveal the initial reasons (*i.e.*,
18 predicate) for an FBI counterterrorism investigation of a particular person (including in
19 Operation Flex), any information obtained during the course of such an investigation, and
20 the status and results of the investigation. This category includes any information
21 obtained from the U.S. Intelligence Community related to the reasons for an
22 investigation.” (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶ 15.) Third, the FBI seeks to
23 protect “[i]nformation that could tend to reveal whether particular sources and methods
24 were used in a counterterrorism investigation of a particular subject, including in
25 Operation Flex,” and “previously undisclosed information related to whether court-
26 ordered searches or surveillance, confidential human sources, and other investigative
27 sources and methods were used in a counterterrorism investigation of a particular person,
28 the reasons such methods were used, the status of the use of such sources and methods,

1 and any results derived from such methods.” (Holder Decl. ¶ 4; Pub. Giuliano Decl. ¶
2 15.)

3
4 Beyond the Government’s descriptions of these categories of information in its
5 public declarations, the Court heavily relies upon the classified declarations and
6 supplemental memorandum to determine whether disclosure of the information described
7 above could reasonably be expected to cause significant harm to national security. In
8 making this determination, the Court assumes the “ ‘special burden to assure itself that an
9 appropriate balance is struck between protecting national security matters and preserving
10 an open court system.’ ” *Jeppesen Dataplan*, 614 F.3d at 1081 (quoting *Al-Haramain*,
11 507 F.3d at 1203); *see also El-Masri*, 479 F.3d at 304 (“This inquiry is a difficult one, for
12 it pits the judiciary’s search for truth against the Executive’s duty to maintain the nation’s
13 security.”). On the one hand, the Court “acknowledge[s] the need to defer to the
14 Executive on matters of foreign policy and national security and surely cannot
15 legitimately find [itself] second guessing the Executive in this arena.” *Jeppesen*
16 *Dataplan*, 614 F.3d at 1081–82; *see also El-Masri*, 479 F.3d at 305 (“In assessing the risk
17 that such a disclosure [of state secrets] might pose to national security, a court is obliged
18 to accord the ‘utmost deference’ to the responsibilities of the executive branch.” (quoting
19 *United States v. Nixon*, 418 U.S. 683, 710 (1974)). On the other hand, “ ‘the state secrets
20 doctrine does not represent a surrender of judicial control over access to the courts.’ ”
21 *Jeppesen Dataplan*, 614 F.3d at 1082 (quoting *El-Masri*, 479 F.3d at 312); *see also*
22 *Reynolds*, 345 U.S. at 9–10 (“Judicial control over the evidence in a case cannot be
23 abdicated to the caprice of executive officers.”) Rather, the Court has the obligation “to
24 ensure that the state secrets privilege is asserted no more frequently and sweepingly than
25 necessary,” by critically examining the instances of its invocation, *Ellsberg v. Mitchell*,
26 709 F.2d 51, 58 (D.C. Cir. 1983), with “a very careful, indeed a skeptical, eye, and not to
27 accept at face value the government’s claim or justification of privilege,” *Al-Haramain*,
28 507 F.3d at 1203. *See also Jeppesen Dataplan*, 614 F.3d at 1082. But the Court cannot

1 delve so deeply that it discloses the very information the privilege is meant to protect.
2 *Reynolds*, 345 U.S. at 8 (“Too much judicial inquiry into the claim of privilege would
3 force disclosure of the thing the privilege is meant to protect, while a complete
4 abandonment of judicial control would lead to intolerable abuses.”)
5

6 The Court has thoroughly and skeptically examined the Government’s public and
7 classified submissions. In particular, the Court has critically scrutinized the Attorney
8 General’s classified declarations and the classified memorandum—which are
9 comprehensive and detailed—since they were submitted for the Court’s *ex parte*, *in*
10 *camera* review in August and November 2011. The Court is convinced that the subject
11 matter of this action, Operation Flex, involves intelligence that, if disclosed, would
12 significantly compromise national security. The Court is further convinced that litigation
13 of this action would certainly require or, at the very least, greatly risk disclosure of secret
14 information, such that dismissal at this stage of the proceeding is required. This is
15 because, as described more fully below, the Government will inevitably need the
16 privileged information to defend against Plaintiffs’ core allegation that Defendants
17 conducted an indiscriminate “dragnet” investigation and gathered information on
18 Plaintiffs and Muslims in Southern California based on their religion. (*See infra* Part
19 IV.C.)
20

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

1 while some of the general facts of Operation Flex are public knowledge, the facts
2 required to *litigate* the action—*e.g.*, to defend against Plaintiffs’ claims of indiscriminate
3 targeting of Muslims—requires disclosure of information that is classified and privileged.
4 *El Masri*, 479 F.3d at 308 (“[F]or purposes of the state secrets analysis, the ‘central facts’
5 and ‘very subject matter’ of an action are those facts that are essential to prosecuting the
6 action or defending against it.”) Plaintiffs’ position to the contrary implies an overly
7 rigid understanding of the difference between the *Totten* bar and *Reynolds* privilege that
8 is inconsistent with the Ninth Circuit’s application of the state secrets doctrine. As the
9 *Jeppesen* court indicated, the state secrets analysis under the *Totten* bar converges with its
10 progeny when, as here, the Government requests dismissal at the pleading stage because
11 defense against plaintiff’s claims requires privileged evidence or further litigation of the
12 case would present an unacceptable risk of disclosing state secrets. *Jeppesen Dataplan*,
13 614 F.3d at 1083. (*See infra* Part IV.C.)

14
15 While the Court cannot describe the specific contents of the classified materials—
16 as this would thwart the very purpose of the privilege claim—the Court can make the
17 following observations. In the context of a counterterrorism investigation, subject
18 identification may include information about persons residing in the United States or
19 abroad, such as Afghanistan, Lebanon, the Palestinian Territories, Yemen, and other
20 regions in the Middle East, whom law enforcement has and has not decided to investigate
21 depending on their nexus to terrorist organizations, such as al Qaeda, the Taliban,
22 Hezbollah, and Hamas. Subjects and their associates may also be investigated because
23 they are suspected of or involved in the recruitment, training, indoctrination, or
24 radicalization of individuals for terrorist activities or fundraising for terrorist
25 organizations. More directly, individuals subjected to counterterrorism investigations
26 may be involved in plotting terrorist attacks. In the nearly eleven years that have passed
27 since September 11, 2001, Islamic extremists have continued to plot and attempt to carry
28 out numerous terrorist attacks both on U.S. soil and abroad against U.S. targets and allies.

1 Such attacks are not abstract events born out of fear, but are real and insidious. The
2 Daily Beast reported that as of September 8, 2011, “there have been at least 45 jihadist
3 terrorist-attack plots against Americans since 9/11—each of them thwarted by a
4 combination of intelligence work, policing and citizen participation.” John Avlon, *Forty-*
5 *Five Foiled Terror Plots Since 9/11*, Daily Beast (Sept. 8, 2011),
6 [http://www.thedailybeast.com/articles/2011/09/08/9-11-anniversary-45-terror-plots-](http://www.thedailybeast.com/articles/2011/09/08/9-11-anniversary-45-terror-plots-foiled-in-last-10-years.html)
7 [foiled-in-last-10-years.html](http://www.thedailybeast.com/articles/2011/09/08/9-11-anniversary-45-terror-plots-foiled-in-last-10-years.html). The article notes that “these are just the plotted attacks that
8 we know about through public documentation” and that “the real number of credible
9 plots is no doubt much higher.” *Id.* Examples of recent, known terrorist attempts include
10 the September 2009 scheme by Najibullah Zazi, who was arrested for plotting to attack
11 the New York City subway system, as well as the December 2009 failed attempt by Umar
12 Farouk Abdulmutallab to bomb Northwest Flight 253 to Chicago and the May 2010
13 failed attempt of Faisal Shazad to detonate a car bomb in Times Square. (*See Pub.*
14 *Giuliano Decl.* ¶¶ 8–9.) Subjects and their associates may be further investigated because
15 they have ties to homegrown violent extremists who do not necessarily receive guidance
16 from terrorist groups overseas but may be inspired by the global jihadist movement to
17 commit violent acts inside the United States. Such was the case for a group of armed
18 men who were arrested before they could execute their plot to kill people inside a
19 military recruiting center in Santa Monica, California, on September 11, 2005, and then
20 later open fire on families outside of temple during Yom Kippur in West Los Angeles.
21 (*See id.* ¶ 10.)

22
23 Disclosure of subjects under investigation would undoubtedly jeopardize national
24 security. This is because persons under investigation would be alerted to the FBI’s
25 interest in them and cause them to flee, destroy evidence, or alter their conduct so as to
26 avoid detection, which would seriously impede law enforcement’s and intelligence
27 officers’ ability to determine their location or gain further intelligence on their activities.
28 (*Holder Decl.* ¶ 6; *Pub. Giuliano Decl.* ¶ 23.) Disclosure of those *not* under investigation

1 by the FBI is, likewise, dangerous because individuals who desire to commit terrorist acts
2 may then be motivated to do so upon discovering that they are not being monitored.
3 Information about who is being investigated while the status of others are unconfirmed
4 may be manipulated by individuals and terrorist groups to discover whether they or any
5 of their members are being investigated. (Holder Decl. ¶ 7; Pub. Giuliano Decl. ¶ 24.)
6

7 The second and third categories of information necessarily overlap with the first.
8 The reasons and results of counterterrorism investigations may include the identities of
9 human sources, such as confidential informants or undercover agents and officers (other
10 than Monteilh); existent or suspected links between individuals and terrorist
11 organizations; the results of surveillance efforts; and information shared among law
12 enforcement and other government agencies. This category of evidence will also likely
13 involve information about the status of the investigation—whether a particular
14 investigation is open or closed—or the substantive details of the investigations
15 themselves. With regard to the third category, this is likely to include information similar
16 to the first and second categories, such as what, if any, confidential human sources
17 besides Monteilh were used; whether court-authorized searches or surveillance occurred,
18 such as wire taps and monitoring of electronic communication; whether the investigations
19 involved undercover activity or physical surveillance; and whether interviews with
20 suspects and their associates were conducted. The disclosure of the reasons and results of
21 counterterrorism investigations would unquestionably compromise national security
22 because it would reveal to those involved in plotting terrorist activities what the FBI
23 knows and does not know about their plans and thereby enable them to evade detection.
24 (Holder Decl. ¶ 9; Pub. Giuliano Decl. ¶ 29.) The disclosure of the methods and sources
25 would endanger national security because it could reveal the identities of particular
26 subjects and the steps taken by the FBI in counterterrorism matters, thereby effectively
27 disclosing a road map to adversaries on how the FBI detects and prevents terrorist
28 activities. (Holder Decl. ¶ 10; Pub. Giuliano Decl. ¶ 31.)

1 Aside from these explanations, the Court cannot and need not give any further
2 details with regard to the contents of the classified materials. *See Kasza*, 133 F.3d at
3 1169 (concluding that *in camera* review of classified declarations “was an appropriate
4 means to resolve the applicability and scope of the state secrets privilege,” and “[n]o
5 further disclosure or explanation is required”). The Court, however, is thoroughly
6 convinced that the Government has described, in sufficient detail, the nature of the
7 privileged information and reasons why its disclosure would compromise national
8 security in its classified filings. Plaintiffs no doubt are frustrated that the Court is
9 precluded from giving any more specifics. But “[a]n inherent feature of the state secrets
10 privilege . . . is that the party against whom it is asserted will often not be privy to the
11 information that the Executive seeks to protect.” *El-Masri*, 479 F.3d at 312. While the
12 Government must persuade the Court with “[s]ufficient detail” that their assertion of the
13 privilege is warranted, *Al-Haramain*, 507 F.3d at 1203, it has no obligation to divulge any
14 details of the privileged matter to Plaintiffs. (*See* Pls. Opp’n to Gov’t, at 31 n.17
15 (criticizing the Government’s public declarations for not describing the alleged privileged
16 information with sufficient specificity). Nevertheless, Plaintiffs’ unfamiliarity with the
17 classified materials’ explanation for the privilege does not imply that “no such
18 explanation was required,” or that the Court’s “ruling was simply an unthinking
19 ratification of a conclusory demand by the executive branch.” *El-Masri*, 479 F.3d at 312.

20 21 **C. Consequences of the Privilege Claim**

22
23 If the court sustains a claim of privilege, then “ ‘the ultimate question to be
24 resolved is how the matter should proceed in light of the successful privilege claim.’ ”
25 *Jeppesen Dataplan*, 614 F.3d at 1080, 1082 (quoting *Al-Haramain*, 507 F.3d at 1202).
26 Ordinarily, a successful claim of the privilege may simply entail excluding or walling off
27 the secret evidence. *Id.* at 1082. But in some instances, as here, application of the
28 privilege may require dismissal of the case. *Id.* at 1083. Dismissal is appropriate in cases

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

16 17 **1. Privileged Information Needed for Defense**

18
19 Dismissal of all of Plaintiffs’ claims, aside from their FISA claim, is required
20 because the privileged information gives Defendants a valid defense. *Jeppesen*
21 *Dataplan*, 614 F.3d at 1083. This analysis of the *Reynolds* privilege necessarily
22 coincides with the *Totten* bar, which permits dismissal of an action at the outset if the
23 very subject matter of the action is a state secret. *Reynolds*, 345 U.S. at 11 n.26. The key
24 test is not whether the general subject matter of Operation Flex is a state secret, but
25 whether this case can be “*litigated* without threatening the disclosure of such state
26 secrets.” *El-Masri*, 479 F.3d at 308. “Subject matter” of an action means “those facts
27 that are essential to prosecuting the action or *defending* against it.” *Id.* (emphasis added);
28 *see also id.* at 309–11 (affirming dismissal of action under the *Reynolds* privilege because

1 defendants needed privileged information related to CIA intelligence operations to defend
2 itself against plaintiff’s claims); *Kasza*, 133 F.3d at 1166 (stating that dismissal is proper
3 “if the privilege deprives the *defendant* of information that would otherwise give the
4 defendant a valid defense to the claim” (citation and quotes omitted)).

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

19
20 Plaintiffs contend that they do not need privileged information to prove their
21 discrimination claims against Defendants. (Pls. Opp’n to Gov’t, at 37.) The Court does
22 not speculate on what Plaintiffs already have in their possession and whether that is
23 enough to prove their claims at this stage of the proceeding. But even assuming that
24 Plaintiffs do not require privileged information to establish their claims, the Court is
25 persuaded that privileged information provides essential evidence for Defendants’ full
26 and effective *defense* against Plaintiffs’ claims—namely, showing that Defendants’
27 purported “dragnet” investigations were not indiscriminate schemes to target Muslims,
28 but were properly predicated and focused. Doing so would require Defendants to

1 summon privileged evidence related to Operation Flex, including the subjects who may
2 or may not have been under investigation, the reasons and results of those investigations,
3 and their methods and sources. Additionally, even if Plaintiffs can successfully show that
4 Defendants' actions substantially burdened their exercise of religion with nonprivileged
5 information, defense against Plaintiffs' First Amendment claims entails analysis of
6 whether the Government had a "compelling state interest" and its actions were "narrowly
7 tailored" to achieve that interest. *Church of the Lukumi Babalu Aye, Inc. v. City of*
8 *Hialeah*, 508 U.S. 520, 546 (1993); *see also Navajo Nation v. United States Forest Serv.*,
9 535 F.3d 1058, 1068 (9th Cir. 2008) ("[S]hould the plaintiff establish a substantial burden
10 on his exercise of religion [for a RFRA claim], the burden of persuasion shifts to the
11 government to prove that the challenged government action is in furtherance of a
12 'compelling governmental interest' and is implemented by 'the least restrictive
13 means.'"). These are fact-intensive questions that necessitate a detailed inquiry into the
14 nature, scope, and reasons for the investigations under Operation Flex. Moreover, with
15 regard to Plaintiffs' FTCA claim, the United States may have a valid defense under the
16 discretionary function exception, *Sabow v. United States*, 93 F.3d 1445, 1451 (9th Cir.
17 1996), which requires the Court to determine "whether the challenged acts . . . are of the
18 nature and quality that Congress intended to shield from tort liability." *United States v.*
19 *Varig Airlines*, 467 U.S. 797, 813 (1984); *see also Dichter-Mad Family Partners, LLP v.*
20 *United States*, 707 F. Supp. 2d 1016, 1018–19 (C.D. Cal. 2010). To establish that this
21 defense applies to the Government's counterterrorism investigations that purportedly
22 violated Plaintiffs' constitutional rights, the Government must marshal facts that fall
23 within the three privileged categories of information related to Operation Flex.¹¹

24
25 ¹¹ Plaintiffs further argue that the Government misunderstands the nature of their religious
26 discrimination claim, which they assert does not require proof that religion is the "sole" reason for their
27 having been targeted for surveillance, but rather that religion was "a" reason that they were targeted.
28 Plaintiffs argue that their essential claim is that religion should be treated like race for the purposes of
anti-discrimination law in that its use should always be justified by strict scrutiny. (Pls. Opp'n to Gov't,
at 21.) As a preliminary matter, Plaintiffs' characterization of their own allegation contradicts the
express language in their FAC. (*See* FAC ¶ 86 (alleging that the FBI Agents' instructions to Monteilh

2. Inseparable from Privileged Information

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

ensured that “Plaintiffs and numerous other people were surveilled *solely* due to their religion”) (emphasis added).) Regardless of the semantics used, however, for the purpose of the state secrets analysis, there is little difference between alleging that Plaintiffs were targeted because of their religion or solely based on their religion. Defense against the claim that Defendants targeted Plaintiffs because of their religion requires the Government to draw on privileged information to show that the investigations were proper and narrowly targeted for a legitimate purpose.

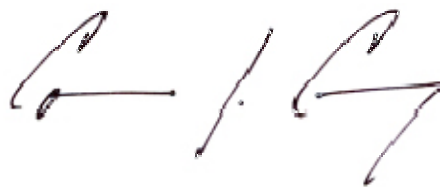
1 Here, as in *Jeppesen Dataplan* and *Kasza*, the subject matter of this case,
2 Operation Flex, involves both privileged and nonprivileged information, which cannot be
3 separated as a practical matter. Indeed, Operation Flex comprises only a small part of the
4 classified mosaic in the FBI's larger counterterrorism investigations, which predate and
5 go beyond Monteilh's source work. The effort to separate privileged from nonprivileged
6 information—even with the protective procedures available to the Court—presents an
7 unjustifiable risk of disclosing state secrets. As the Ninth Circuit observed,
8 “[a]dversarial litigation, including pretrial discovery of documents and witnesses and the
9 presentation of documents and testimony at trial, is inherently complex and
10 unpredictable.” *Jeppesen Dataplan*, 614 F.3d at 1089. “Although district courts are well
11 equipped to wall off isolated secrets from disclosure, the challenge is exponentially
12 greater in exceptional cases like this one, where the relevant secrets are difficult or
13 impossible to isolate and even efforts to define a boundary between privileged and
14 unprivileged evidence would risk disclosure by implication.” *Id.* In such rare
15 circumstances, as here, the risk of disclosure that further litigation would engender cannot
16 be averted through protective orders or restrictions on testimony. *Id.* This is true even as
17 to Plaintiffs' Fourth Amendment claim because it is impossible to excise the facts
18 directly related to this claim from the factual context of Operation Flex as a whole, and
19 that context forms an important background for a finder of fact to consider in her
20 analysis. While this case is only at the pleading stage and Plaintiffs have not yet
21 propounded any discovery requests, (Arulanantham Decl. ¶ 2), Defendants need not wait
22 before discovery or evidentiary disputes are at issue to assert the privilege for dismissal.
23 *Jeppesen Dataplan*, 614 F.3d at 1081 (“Courts are not required to play with fire and
24 chance further disclosure—inadvertent, mistaken, or even intentional—that would defeat
25 the very purpose for which the privilege exists.” (quoting *Sterling v. Tenet*, 416 F.3d 338,
26 344 (4th Cir. 2005)). Accordingly, because further litigation of this action would create
27 “an unjustifiable risk of revealing state secrets” related to the FBI's counterterrorism
28 investigations, dismissal of Plaintiffs' claims is warranted. *Id.* at 614 F.3d at 1088.

1 **V. CONCLUSION**

2
3 The state secrets privilege strives to achieve a difficult compromise between the
4 principles of national security and constitutional freedoms. The state secrets privilege
5 can only be invoked and applied with restraint, in narrow circumstances, and infused with
6 judicial skepticism. Yet, when properly invoked, it is absolute—the interest of protecting
7 state secrets cannot give way to any other need or interest. Navigating through the
8 narrow straits of the state secrets privilege has not been an easy or enviable task for the
9 Court. In the context of the Executive’s counterterrorism efforts engendered by 9/11, the
10 Court has been confronted with the difficult task of balancing its obligation to defer to the
11 Executive in matters of national security with its duty to promote open judicial inquiry.
12 Too much deference would short-circuit constitutional liberties while too much judicial
13 inquiry would risk disclosure of information that would jeopardize national security. In
14 struggling with this conflict, the Court is reminded of the classic dilemma of Odysseus,
15 who faced the challenge of navigating his ship through a dangerous passage, flanked by a
16 voracious six-headed monster, on the one side, and a deadly whirlpool, on the other.
17 Odysseus opted to pass by the monster and risk a few of his individual sailors, rather than
18 hazard the loss of his entire ship to the sucking whirlpool. Similarly, the proper
19 application of the state secrets privilege may unfortunately mean the sacrifice of
20 individual liberties for the sake of national security. *El-Masri*, 479 F.3d at 313 (“[A]
21 plaintiff suffers this reversal not through any fault of his own, but because his personal
22 interest in pursuing his civil claim is subordinated to the collective interest in national
23 security.”); *Sterling*, 416 F.3d at 348 (“[T]here can be no doubt that, in limited
24 circumstances . . . the fundamental principle of access to court must bow to the fact that a
25 nation without sound intelligence is a nation at risk.”); *Fitzgerald v. Penthouse Int’l, Ltd.*,
26 776 F.2d 1236, 1238 n.3 (4th Cir. 1985) (“When the state secrets privilege is validly
27 asserted, the result is unfairness to individual litigants—through the loss of important
28 evidence or dismissal of a case—in order to protect a greater public value.”)

1 The Court recognizes the weight of its conclusion that Plaintiffs must be denied a
2 judicial forum for their claims. The Court does not reach its decision today lightly, but
3 does so only reluctantly, after months of careful review of the parties' submissions and
4 arguments, particularly the Government's *in camera* materials upon which the Court
5 heavily relies. Plaintiffs raise the specter of *Korematsu v. United States*, 323 U.S. 214
6 (1944), and protest that dismissing their claims based upon the state secrets privilege
7 would permit a "remarkable assertion of power" by the Executive, and that any practice,
8 no matter how abusive, may be immunized from legal challenge by being labeled as
9 "counterterrorism" and "state secrets." (Pls. Opp'n to Gov't, at 20, 41-42.) But such a
10 claim assumes that courts simply rubber stamp the Executive's assertion of the state
11 secrets privilege. That is not the case here. The Court has engaged in rigorous judicial
12 scrutiny of the Government's assertion of privilege and thoroughly reviewed the public
13 and classified filings with a skeptical eye. The Court firmly believes that after careful
14 examination of all the parties' submissions, the present action falls squarely within the
15 narrow class of cases that require dismissal of claims at the outset of the proceeding on
16 state secret grounds. Accordingly, all of Plaintiffs' causes of action against Defendants,
17 aside from their FISA claim, are DISMISSED.

18
19
20 DATED: August 14, 2012



21
22 CORMAC J. CARNEY
23 UNITED STATES DISTRICT JUDGE
24
25
26
27
28