

1 **II. (U) THE UNITED STATES HAS PROPERLY ASSERTED THE STATE**
2 **SECRETS PRIVILEGE IN THIS CASE.**

3 (U) The United States has properly asserted the state secrets privilege in this case. The
4 Director of National Intelligence, J. Michael McConnell, who bears statutory authority as head
5 of the United States Intelligence Community to protect intelligence sources and methods, *see* 50
6 U.S.C. § 403-1(i)(1),¹⁴ has formally asserted the state secrets privilege after personal
7 consideration of the matter. *See Reynolds*, 345 U.S. at 7-8. DNI McConnell has submitted an
8 unclassified declaration and an *in camera, ex parte* classified declaration, both of which state
9 that the disclosure of the intelligence information, sources, and methods described therein would
10 cause exceptionally grave harm to the national security of the United States. See Public and *In*
11 *Camera* Declarations of J. Michael McConnell, Director of National Intelligence. Based on this
12 assertion of privilege by the head of the United States Intelligence Community, the
13 Government's claim of privilege has been properly lodged.

14 (U) As set forth in the following section, the information at issue in the Government's
15 privilege assertion is central to the resolution of this case and the harms to national security that
16 would result from its disclosure require dismissal of the action.

17 **III. (U) INFORMATION SUBJECT TO THE STATE SECRETS PRIVILEGE IS**
18 **NECESSARY TO ADJUDICATE PLAINTIFFS' CLAIMS AND, THUS, THIS**
19 **ACTION CANNOT PROCEED.**

20 (U) As noted above, once the state secrets privilege is asserted, the Court must evaluate
21 the consequences of that assertion on the case. Here, state secrets are "so central to the subject
22 matter of the litigation that any attempt to proceed will threaten disclosure of the privileged
23 matters." *Fitzgerald*, 776 F.2d at 1241-42. Indeed, Plaintiffs' cannot prove their standing or
24 claims, and Defendants cannot present a full defense, without the privileged information. *See*

25 ¹⁴ (U) See 50 U.S.C. § 401a(4) (including the National Security Agency in the United States
26 "Intelligence Community").

1 *Kasza*, 133 F.3d at 1166. Specifically, adjudicating each of Plaintiffs' claims would necessarily
2 require: (1) confirming or denying the existence of a NSA-Verizon relationship with respect to
3 the particular alleged activities; (2) confirming or denying that the named Plaintiffs have been
4 subject to any alleged activities; (3) proving that the content surveillance program authorized by
5 the President after 9/11 was not a dragnet of domestic communications as alleged; (4)
6 confirming or denying the existence of the alleged communications records activities; and (5)
7 disclosing the nature and scope of any such alleged activities, including the precise nature of the
8 activities, how they were conducted, why they were conducted, when they were conducted and
9 for how long, and the intelligence value of the activities. Because such information cannot be
10 disclosed without causing exceptionally grave damage to the national security, every step in this
11 case—either for Plaintiffs to prove their claims, for Defendants to defend them, or for the United
12 States to represent its interests—runs into privileged information.

13 **A. (U) Whether or Not MCI/Verizon Has a Relationship with the NSA is a**
14 **State Secret Necessary to Decide This Case.**

15 (U) The first and most obvious matter at issue is whether MCI and Verizon have assisted
16 the NSA in any alleged intelligence activities at issue. A confirmation or denial of the alleged
17 relationship, however, is precluded by long-standing authority, not only under the state secrets
18 privilege, but under the *Totten* doctrine as well. These are closely related but distinct grounds
19 for dismissing Plaintiffs' claims.

20 **1. (U) The *Totten* Doctrine Requires Dismissal of this Action to Protect**
21 **Whether or Not MCI/Verizon Has a Relationship with the NSA.**

22 (U) In the first instance, this case squarely falls within the *Totten/Tenet* rule of dismissal.
23 In *Totten v. United States*, the Supreme Court held that public policy forbade a self-styled Civil
24 War spy from suing the United States to enforce an alleged secret espionage agreement. In
25 rejecting the claim of the alleged spy's estate that the United States had refused to pay him under
26 a contract he allegedly entered into with President Lincoln to spy on Confederate military

1 operations, the Supreme Court held that “[t]he service stipulated by the contract was a secret
2 service; the information sought was to be obtained clandestinely, and was to be communicated
3 privately; the employment and the service were to be equally concealed.” *Totten*, 92 U.S. at 107.

4 The Court added:

5 Both employer and agent must have understood that the lips of the other were to
6 be forever sealed respecting the relation of either to the matter. This condition of
7 the engagement was implied from the nature of the employment, and is implied in
8 all secret employments of the Government in time of war, or upon matters
affecting our foreign relations, where a disclosure of the service might
compromise or embarrass our Government in its public duties, or endanger the
person or injure the character of the agent.

9 *Id.* For this reason, the Court held that “public policy forbids the maintenance of any suit in a
10 court of justice, the trial of which would inevitably lead to the disclosure of matters which the
11 law itself regards as confidential, and respecting which it will not allow the confidence to be
12 violated.” *Id.*

13 (U) This precise principle was reaffirmed by the Supreme Court in *Tenet v. Doe*. In
14 *Tenet*, alleged former spies sued the United States and the Director of the Central Intelligence
15 Agency (CIA) claiming that the Government had failed to provide the assistance it had promised
16 in return for their espionage services. *See* 544 U.S. at 3-5. The Supreme Court held that the
17 Court of Appeals was “quite wrong” in holding that *Totten* was limited to a mere “contract rule”
18 prohibiting breach-of-contract claims seeking to enforce the terms of espionage agreements but
19 not barring other claims based on due process or estoppel theories. *Id.* at 9. Instead, the Court
20 reiterated that “public policy forbids the maintenance of *any* suit . . . which would inevitably
21 lead to the disclosure of [confidential] matters.” *Id.* (quoting *Totten*, 92 U.S. at 107) (emphasis
22 added). The Court thus held that “*Totten* precludes judicial review in cases such as respondents’
23 where success depends upon the existence of their secret espionage relationship with the
24 Government.” *Id.*

25 (U) Indeed, the *Tenet* Court went on to note that the *Totten* rule was not merely an “early
26

1 expression” of the state secrets evidentiary privilege under *Reynolds*, but a “categorical bar” to
2 such claims. Specifically distinguishing the privilege, the Court held that *Reynolds* “in no way
3 signaled our retreat from *Totten’s* broader holding that lawsuits premised on alleged espionage
4 agreements are altogether forbidden.” *Id.*¹⁵ Noting that “[e]ven a small chance that some court
5 will order disclosure of a source’s identity could well impair intelligence gathering and cause
6 sources to ‘close up like a clam,’” *Tenet*, 544 U.S. at 11 (quoting *CIA v. Sims*, 471 U.S. 159, 175
7 (1985)), the Court concluded that the “possibility that a suit may proceed and an espionage
8 relationship may be revealed, if the state secrets privilege is found not to apply, is unacceptable.”
9 *Id.*

10 (U) In this case, the sum and substance of Plaintiffs’ allegations are that MCI and
11 Verizon have “a secret espionage relationship with the Government.” *Totten*, 92 U.S. at 107. An
12 adjudication of Plaintiffs’ claims would necessarily require either confirming or denying the
13 existence of that relationship. Accordingly, dismissal of this action is required by the
14 *Totten/Tenet* categorical bar to litigation that threatens to disclose alleged covert relationships.
15 The *Hepting* decision recognizes that a case such as this “involves an alleged covert
16 relationship” between the Government and telecommunications carrier, but the Court
17 nevertheless held that *Totten* and *Tenet* pose no bar for two reasons. First the Court held that
18 *Totten* is limited to claims seeking to enforce an espionage relationships. Second, the Court
19 found that AT&T and the Government had already effectively admitted the relationship. Neither
20 conclusion should apply here.

21 _____
22 ¹⁵ (U) The *Tenet* Court observed that *Reynolds* itself refutes this very suggestion because
23 *Reynolds* cites *Totten* as a case “where the very subject matter of the action, a contract to
24 perform espionage, was a matter of state secret,” and declares that such a case was to be
25 “dismissed on the pleadings without ever reaching the question of evidence, since it was so
26 obvious that the action should never prevail over the privilege.” *Reynolds*, 345 U.S. at 11
(emphasis added).

1 (U) As to the scope of *Totten*, the Court held that “[t]he implicit notion in *Totten* was one
2 of equitable estoppel: one who agrees to conduct covert operations impliedly agrees not to reveal
3 the agreement even if the agreement is breached.” *Hepting*, 439 F. Supp. 2d at 991. In the
4 Court’s view, because “AT&T, the alleged spy, is not the plaintiff here,” plaintiffs have “made
5 no agreement with the government and are not bound by any implied covenant of secrecy.” *Id.*
6 With respect, the Court misread *Totten* and *Tenet*, neither of which turned on an “implicit”
7 equitable estoppel theory. Rather, the Supreme Court explained explicitly in *Tenet* that *Totten*’s
8 rule “was not so limited,” see *Tenet*, 544 U.S. at 9 (emphasis added), and that *any suit* that would
9 inevitably lead to the disclosure of confidential information must be dismissed, see *id.* (emphasis
10 added). Of course, disclosure of a classified relationship would cause the same harm to national
11 security whether or not the plaintiff was a party to the alleged relationship. Because Plaintiffs’
12 action here hinges on the existence of an asserted secret espionage relationship between MCI
13 and/or Verizon and the NSA, *Totten* and *Tenet* are directly applicable.

14 (U) *Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139
15 (1981)—cited by the Supreme Court in *Tenet*, 544 U.S. at 9—confirms the error in limiting
16 *Tenet* and *Totten* to an “implicit” equitable estoppel theory. In *Weinberger*, the Supreme Court
17 invoked *Totten* in dismissing a challenge under the National Environmental Protection Act
18 (“NEPA”), where the determination of whether the Navy complied with NEPA was held to be
19 beyond judicial scrutiny because, “due to national security reasons” the Navy could not admit or
20 deny the central fact at issue in that suit as to whether it proposed to store nuclear weapons at a
21 facility. See 454 U.S. at 147. Thus, the Supreme Court in *Weinberger* applied the *Totten* rule
22 completely outside the context of an asserted espionage agreement, and precluded a lawsuit by
23 someone with no alleged contractual relationship with the Government. *Weinberger*
24 underscores that *Totten* is not a rule of “equitable estoppel.”

25 (U) The Fourth Circuit’s recent ruling in *El-Masri* is also instructive. There, as in this
26

1 case, the plaintiff, who was not a party to an alleged espionage relationship, sued corporate and
2 individual defendants, alleging their participation in secret and unlawful Government activity.
3 The Fourth Circuit affirmed dismissal of the case on state secrets grounds, explaining that, for
4 the litigation to proceed, plaintiff “would have to demonstrate the existence and details of
5 [Government] espionage contracts, an endeavor practically indistinguishable from that
6 categorically barred by *Totten* and *Tenet*.” *El-Masri*, ___ F.3d at ___, 2007 WL 625130 at *9.

7 (U) Beyond this, the Court’s conclusion in *Hepting* that “unlike the clandestine spy
8 arrangements in *Tenet* and *Totten*, AT&T and the government have for all practical purposes
9 already disclosed that AT&T assists the government in monitoring communication content,” is
10 also flawed for several reasons. *Hepting*, 439 F. Supp. 2d at 991. First, the Government’s mere
11 acknowledgment of a program (the TSP) not even challenged in *Hepting* (or here) surely cannot
12 be read as an acknowledgment of any other program, nor can it be read as an acknowledgment of
13 AT&T or Verizon’s participation in any program. Nor does the simple fact of AT&T’s size or
14 publicly-stated willingness to assist generally with law enforcement matters provide any basis to
15 conclude that AT&T assisted the NSA with any specific foreign intelligence program. *Totten*
16 and *Tenet* are clear that the subject of a classified espionage relationship is *categorically barred*
17 from litigation, and thus the very process undertaken by the Court of sifting through public
18 statements to determine *whether* the case could proceed under *Totten* itself conflicted with that
19 the rule established in that case.

20 (U) Furthermore, any public statements by the private party purportedly involved in the
21 alleged relationship (AT&T in *Hepting* and Verizon here) are plainly irrelevant under *Totten* and
22 *Tenet*. Indeed, unlike here, the plaintiffs in both of those cases would have *known* about their
23 connection to the alleged espionage relationship. Nonetheless, the Supreme Court held that such
24 relationships are not permissible topics of litigation. Where suits concerning alleged espionage
25 relationships are categorically barred even where a party to that alleged relationship—an actual
26

1 *witness* to the alleged matter—seeks to disclose its existence, it cannot be the case that parties
2 with no actual knowledge can force disclosure of whether such a relationship existed. Under the
3 Court’s reasoning, if AT&T or Verizon sued the Government alleging that they had assisted in
4 classified NSA activities and seeking to enforce a government contract with respect to such
5 activities, the matter would have to be dismissed to protect national security, whereas a party
6 with *no knowledge* of that alleged relationship could sue to force its very disclosure. That
7 outcome is inconsistent with the purpose of the *Totten/Tenet* doctrine: to avoid disclosing
8 information that public policy requires be maintained as confidential due to national security
9 reasons, including impairing the nation’s intelligence activities. *See Tenet*, 544 U.S. at 9.

10 **2. (U) The State Secrets Privilege Also Requires Dismissal of this Action to**
11 **Protect Whether or Not MCI/Verizon Assisted the NSA in the Alleged**
12 **Activities.**

13 (U) Even if the categorical bar to suit under the *Tenet/Totten* doctrine did not apply here,
14 the state secrets privilege provides a distinct and independent ground for dismissing Plaintiffs’
15 claims against the Verizon Defendants. The question presented by the state secrets privilege is
16 whether facts confirming or denying Verizon’s alleged assistance to the NSA with respect to the
17 alleged activities are necessary to decide the case but would cause harm to national security if
18 disclosed. If that is so, the case cannot proceed. Here, of course, it cannot be disputed that
19 disclosure of whether or not Verizon assisted the NSA is essential to proceeding. Indeed, it is a
20 key element of every one of Plaintiffs’ claims. The Government has not confirmed or denied
21 whether Verizon assisted with any of the alleged activities, and no grounds exist for finding that
22 such information may be disclosed in this case in the face of the harms to national security
23 identified by the DNI and NSA Director.

24 (U) *Alleged Content Surveillance Dragnet*: With respect to the surveillance of the
25 content of communications, the Government’s acknowledgment of the *existence* of the Terrorist
26 Surveillance Program revealed nothing about whether particular telecommunication companies

1 such as Verizon assisted with that program. The Court's analysis on this point in *Hepting*—that
2 the NSA could not conduct the alleged activities without the assistance of the private
3 sector—was based on the judicially noticed fact that AT&T is a large company. *See* 439 F. Supp.
4 2d at 991-92. But no public facts provide any basis to conclude that only large firms, and not
5 small ones, would have the resources or expertise to furnish any needed assistance (if, indeed,
6 there was any such assistance), or that the Government could not accomplish the alleged
7 surveillance on its own. Similarly, the fact that AT&T has a history of providing some
8 assistance to the Government, including on general law enforcement matters or some
9 unspecified classified contracts, *see id.*, does not mean that the Government requested AT&T's
10 assistance, or that AT&T provided assistance, with respect to the NSA surveillance activities
11 alleged in *Hepting*. Indeed, even considering AT&T's general statements concerning its
12 cooperation with the United States on unspecified projects, no relationship between AT&T and
13 the NSA in connection with any of the activities alleged in *Hepting* has *ever* been confirmed or
14 denied, and the public record provides no basis for inferring whether such a relationship exists.
15 The Court was thus able to state only that "AT&T is assisting the government to implement
16 *some kind* of surveillance program," and "AT&T and the government have *some kind* of
17 intelligence relationship," *see id.* at 994 (emphasis added). Particularly where the Plaintiffs in
18 *Hepting*, as here, are not even challenging the content surveillance program that was
19 acknowledged by the President—the TSP—these conclusions were insufficient to override the
20 judgment of the Director of National Intelligence on a matter of national security as to the harm
21 that would result from confirming or denying an intelligence relationship with respect to specific
22 allegations.

23 (U) The same is true in this case. Whether or not Verizon may have assisted the
24 Government with classified or law enforcement matters in general says nothing about whether it
25 has assisted the NSA in connection with the activities alleged in these cases. Similarly, the
26

1 relative size of Verizon does not by itself indicate assistance as to a particular activity such as
2 the TSP, especially where information about the operation of that activity has not been
3 disclosed.

4 (U) The harms to national security at stake in confirming or denying an alleged
5 intelligence relationship are indeed significant. Revealing whether or not Verizon assists the
6 NSA with specific intelligence activities, for example, would replace speculation with certainty
7 for hostile foreign adversaries who are balancing the risk that a particular channel of
8 communication may not be secure against the need to communicate efficiently. Public
9 McConnell Decl. ¶ 13. The Court itself recognized this concern with respect to the alleged
10 communications records activities, when it observed in *Hepting* that “[a] terrorist who operates
11 with full information is able to communicate more securely and more efficiently than a terrorist
12 who operates in an atmosphere of uncertainty.” *See id.* at 990. The DNI has set forth a more
13 than reasonable basis to conclude that harm to national security would result from the disclosure
14 of whether or not the NSA has worked with Verizon in connection with the alleged activities,
15 and the Court has correctly observed that it is not in a position to second guess the DNI’s
16 judgment regarding a terrorist’s risk preferences—a judgment which might depend on an array
17 of facts not before the Court. *See Hepting*, 439 F. Supp. 2d at 990, 997.

18 (U) Weighed against these considerations is the mere allegation, based on conjecture and
19 media reports, that Verizon must be assisting the NSA with certain alleged intelligence activities
20 without judicial supervision. *See, e.g.*, Master Verizon Complaint ¶¶ 142-62. Such unconfirmed
21 speculation cannot outweigh the DNI’s assertion of privilege and the harms he has identified.
22 The Court has already rejected reliance on information in media reports to undercut a state
23 secrets privilege assertion. *See Hepting*, 439 F. Supp. 2d at 989-90. Indeed, reliance on such
24 reports would improperly place national security decisions in the hands of reporters whose
25 sources often speculate as to government activity and whose reporting in any event will not
26

1 always be presumed accurate or reliable by the public. It would also require the United States to
2 officially confirm or deny such reporting when the government has not previously done so. That
3 outcome would largely eviscerate the state secrets privilege and is contrary to cases that affirm
4 the Government's right to protect national security information if the Government has not
5 officially disclosed the precise information to the public. Even when alleged facts have been the
6 "subject of widespread media and public speculation" based on "[u]nofficial leaks and public
7 surmise," those alleged facts are not actually established in the public domain. *Afshar v.*
8 *Department of State*, 702 F.2d 1125, 1130-31 (D.C. Cir. 1983); *see also Fitzgerald*, 776 F.2d at
9 1242-43 (affirming dismissal because subject was state secret despite published article on the
10 matter); *Edmonds v. FBI*, 272 F. Supp. 2d at 49 (because statements in the press were made by
11 anonymous sources, even documents containing identical information may properly be withheld
12 because "release would amount to official confirmation or acknowledgment of their accuracy").

13 (U) In a case directly on point, the Court in *Terkel* expressly held that the Government
14 had not confirmed or denied involvement by AT&T in the alleged communication records
15 program and that it would "undermine the important public policy underlying the state secrets
16 privilege if the government's hand could be forced by unconfirmed allegations in the press or by
17 anonymous leakers whose disclosures have not been confirmed." *Terkel v. AT&T*, 441 F. Supp.
18 2d at 913-14 (holding that media reports of alleged NSA programs "amount to nothing more
19 than unconfirmed speculation").

20 (U) Similarly, public statements by Verizon itself, *see* Master Verizon Compl.
21 ¶¶ 160-61, are irrelevant to the state secrets privilege inquiry. As the Supreme Court has
22 admonished, the state secrets privilege "belongs to the Government" and cannot be "waived by a
23 private party." *Reynolds*, 345 U.S. at 7; *see Kasza*, 133 F.3d at 1165. Thus, in inquiring
24 whether a relationship had been confirmed or denied, the Court in *Hepting* should have limited
25 itself to authoritative Government statements and should not have looked to statements by other
26

1 persons or entities. As the courts have recognized, “disclosure of information by government
2 officials can be prejudicial to government interests, even if the information has already been
3 divulged from non-government sources.” *Bareford v. General Dynamics Corp.*, 973 F.2d at
4 1144 (5th Cir. 1992).¹⁶

5 (U) *Alleged Communication Records Collection*: With respect to the alleged collection
6 of communication records information, the Court in *Hepting* agreed that the authorized
7 Executive Branch officials have not confirmed this activity, let alone a telecommunication
8 carrier’s assistance in the matter. *See Hepting*, 4430 F. Supp. 2d at 997. And although the Court
9 erred in our view by declining to dismiss this claim in *Hepting* because of the possibility that the
10 Government or telecommunication carriers “might disclose, either deliberately or accidentally,
11 other pertinent information about the communication records program as this litigation
12 proceeds,” and that “such disclosures might make this program’s existence or non-existence no
13 longer a secret,” *id.* at 997-98, nothing warrants proceeding with these allegations in this case.

14 As the Court noted:

15 Revealing that a communications records program exists might encourage that
16 terrorist to switch to less efficient but less detectable forms of communication.
17 And revealing that such a program does not exist might encourage a terrorist to
18 use [a provider’s] services when he would not have done so otherwise.

19 *Hepting*, 439 F. Supp. 2d at 997; *accord Terkel v. AT&T*, 441 F. Supp. 2d at 915 (requiring
20 telecommunications carrier to admit or deny existence of Government request to assist on
21 alleged communications records program would disclose significant information that had not
22 been revealed by other public information). Even a small margin of error may make the
23 difference in protecting national security. Under these circumstances, and in light of the highly

24 ¹⁶ (U) Any effort to use this litigation to ascertain the meaning of Verizon’s statements
25 would plainly require discovery and confirmation of whether and to what extent MCI or
26 Verizon assisted the Government and whether and to what extent the alleged activities even
27 existed—that is, it would require *new and additional* facts that are subject to the state secrets
28 privilege assertion.

1 deferential standard of review under the state secrets privilege, for the Court to conclude based
2 on limited public facts that the Executive Branch must confirm or deny alleged intelligence
3 sources or methods, where such disclosures may pose grave or even unforeseeable
4 consequences, would be misguided and inappropriate.

5
6 **[REDACTED TEXT]**

7
8 * * *

9 (U) Because confirming or denying the alleged relationship between the NSA and the
10 Verizon Defendants could reasonably be expected to cause the harms to national security
11 described by the DNI and NSA Director, and because adjudicating Plaintiffs' claims will
12 necessarily require confirming or denying such a relationship, the case must be dismissed.
13 Dismissal is required regardless of whether the matter is considered to be the "very subject
14 matter" of the case, or because facts concerning the alleged relationship would be needed for
15 Plaintiffs' to make a *prima facie* case or for a defense to be presented. The issue remains the
16 same: facts concerning Verizon's alleged relationship with the NSA must be placed into
17 evidence for this case to proceed, and doing so would plainly harm the national security interests
18 of the United States.

19 **B. (U) Whether or Not Plaintiffs Have Standing Cannot be Established or**
20 **Refuted Without the Disclosure of State Secrets and Harm to National**
21 **Security.**

22 (U) Aside from whether MCI or Verizon had any involvement in the alleged NSA
23 activities, the equally fundamental issue of Plaintiffs' standing cannot be adjudicated without
24 state secrets. As is well known, the Constitution "limits the jurisdiction of federal courts to
25 'Cases' and 'Controversies,'" and "the core component of standing is an essential and
26 unchanging part of th[is] case-or-controversy requirement." *Lujan v. Defenders of Wildlife*, 504

1 U.S. 555, 559-60 (1992). Plaintiffs, of course, bear the burden of establishing standing and
2 must, at an “irreducible constitutional minimum,” demonstrate (1) an injury-in-fact, (2) a causal
3 connection between the injury and the conduct complained of, and (3) a likelihood that the injury
4 will be redressed by a favorable decision. *Id.* In meeting that burden, the named Plaintiffs must
5 demonstrate an actual or imminent—not speculative or hypothetical—injury that is
6 particularized as to them; they cannot rely on alleged injuries to unnamed members of a
7 purported class.¹⁷ Moreover, to obtain prospective relief, Plaintiffs must show that they are
8 “immediately in danger of sustaining some direct injury” as the result of the challenged conduct.
9 *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983); *O’Shea v. Littleton*, 414 U.S. 488,
10 495-96 (1974).¹⁸

11 (U) A plaintiff must demonstrate Article III standing for “each claim he seeks to press,”
12 *DaimlerChrysler Corp. v. Cuno*, 126 S. Ct. 1854, 1867 (2006), and must further establish
13 “prudential” standing by showing that “the constitutional or statutory provision on which [each]
14 claim rests properly can be understood as granting persons in the plaintiff’s position a right to
15 judicial relief.” *Warth*, 422 U.S. at 499-500. To do so, a plaintiff normally “must assert his
16

17 ¹⁷ (U) *See, e.g., Warth v. Seldin*, 422 U.S. 490, 502 (1975) (the named plaintiffs in an action
18 “must allege and show that they personally have been injured, not that injury has been suffered
19 by other, unidentified members of the class to which they belong and which they purport to
represent”).

20 ¹⁸ (U) Standing requirements demand the “strictest adherence” when, like here, constitutional
21 questions are presented and “matters of great national significance are at stake.” *Elk Grove*
22 *Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 11 (2004); *see also Raines v. Byrd*, 521 U.S. 811,
23 819-20 (1997) (“[O]ur standing inquiry has been especially rigorous when reaching the merits
24 of the dispute would force us to decide whether an action taken by one of the other two
25 branches of the Federal Government was unconstitutional.”); *Schlesinger v. Reservists Comm.*
26 *to Stop the War*, 418 U.S. 208, 221 (1974) (“[W]hen a court is asked to undertake constitutional
adjudication, the most important and delicate of its responsibilities, the requirement of concrete
injury further serves the function of insuring that such adjudication does not take place
unnecessarily.”).

27 **Public Memorandum of the United States**
28 **in Support of Motion to Dismiss or for Summary**
Judgment, MDL No. 06-1791-VRW

1 own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of
2 third parties.” *Smelt v. County of Orange*, 447 F.3d 673, 682 (9th Cir. 2006) (quoting *Phillips*
3 *Petroleum Co. v. Shutts*, 472 U.S. 797, 804 (1985)). To advance a statutory claim, a plaintiff
4 must show that his particular injury “fall[s] within ‘the zone of interests to be protected or
5 regulated by the statute’” in question. *Id.* at 683.

6 (U) Here, the state secrets privilege prevents Plaintiffs from establishing, and Defendants
7 from refuting, any injury because it bars proof of whether Plaintiffs have been subject to the
8 alleged surveillance activities.¹⁹ As discussed, the Government’s privilege assertion covers,
9 *inter alia*, any information (1) tending to confirm or deny whether the Plaintiffs were subject to
10 any of the alleged intelligence activities at issue, (2) tending to confirm or deny whether Verizon
11 is involved with particular alleged intelligence activities, and (3) concerning the alleged
12 activities, including program facts demonstrating that the TSP was limited to one-end foreign al
13 Qaeda communications and was not the dragnet that Plaintiffs allege, and facts that would
14 confirm or deny the existence of the alleged communications records activities. *See* Public
15 McConnell Decl. ¶ 16. Without these facts—the disclosure of which would harm national
16 security for reasons explained by the DNI and NSA Director—Plaintiffs cannot establish any
17 alleged injury that is fairly traceable to Verizon.

18 (U) It is important to emphasize the procedural posture of the Government’s pending
19 motions as they pertain to this standing issue. Whether the Plaintiffs can establish their standing

20
21 ¹⁹ (U) The focus herein is on Plaintiffs’ inability to prove standing because it is their burden to
22 demonstrate jurisdiction. *See Lujan*, 504 U.S. at 561. Dismissal of this action, however, is also
23 required for the equally important reason that the MCI and Verizon Defendants and the United
24 States as intervenor would not be able to present any evidence disproving standing on any claim
25 without revealing information covered by the state secrets privilege assertion (*e.g.*, whether or
26 not a particular person’s communications were intercepted). *See Halkin I*, 598 F.2d at 11
(rejecting plaintiffs’ argument that the acquisition of a plaintiff’s communications may be
presumed from the existence of a name on a watchlist, because “such a presumption would be
unfair to the individual defendants who would have no way to rebut it”).

1 is not merely a question to be decided on the pleadings. Regardless of whether Plaintiffs
2 adequately allege injury to get past the pleading stage, the United States, through its motion for
3 summary judgment, has specifically put at issue whether the named Plaintiffs will be able to
4 sustain their burden of *proving* a concrete, personal injury *as a factual matter* in light of the state
5 secrets privilege assertion.²⁰ Given the Government's summary judgment motion, the Plaintiffs
6 cannot rest on general allegations in their complaints, but must be able to set forth specific facts
7 by affidavit or evidence that would support their standing to obtain the relief sought. *See Lewis*
8 *v. Casey*, 518 U.S. 343, 358 (1996) (quoting *Lujan*, 504 U.S. at 561). The issue raised by the
9 Government's motion is whether that will be possible where the DNI has properly asserted
10 privilege over facts tending to confirm or deny the application of alleged intelligence activities to
11 particular individuals, including the named Plaintiffs in this case. Because the DNI has set forth
12 reasonable grounds to protect such information, the facts needed to establish or refute the
13 Plaintiffs' standing cannot be disclosed and the case thus cannot proceed. This is not an issue
14 that can be deferred. If Plaintiffs' claims of injury cannot be proven without disclosing state
15 secrets and harming national security—and we submit they cannot—then judgment must be
16 entered in favor of the Defendants now.

17 (U) In *Hepting*, the United States argued, as it has here, that the plaintiffs would be
18 unable to establish standing absent state secrets. In addressing that issue, the Court referred to
19 its prior conclusion that “the state secrets privilege will not prevent plaintiffs from receiving at
20

21 ²⁰ (U) The Court can dismiss this case on the pleadings under the *Totten/Tenet* rule and the
22 “very subject matter” prong of the state secrets privilege. The Government's summary
23 judgment motion is made in the alternative because, if the Court declines to dismiss on those
24 grounds, the questions of whether the state secrets privilege precludes Plaintiffs from proving
25 their standing or making a *prima facie* case, or Defendants from presenting a defense, are more
26 properly considered as summary judgment questions. *See Zuckerbraun*, 935 F.2d at 547.
Indeed, the Government's summary judgment motion places the burden on Plaintiffs to prove
their standing and to make out a *prima facie* case without state secrets, which they cannot do.

27 Public Memorandum of the United States
in Support of Motion to Dismiss or for Summary
28 Judgment, MDL No. 06-1791-VRW

1 least some evidence tending to establish the factual predicate of the injury-in-fact underlying
2 their claims directed at AT&T's alleged involvement in the monitoring of communication
3 content." 439 F. Supp. 2d at 1001. With respect, the Court's conclusion in *Hepting* as to the
4 impact of the state secrets privilege on the plaintiffs' standing was in error. By focusing solely
5 on the issue of AT&T's alleged involvement, the Court disregarded the critical factual issue
6 related to standing: whether the *individual plaintiffs* had in fact been subjected to the alleged
7 intelligence activities. That issue exists apart from whether AT&T had any involvement in the
8 alleged activities, because if the plaintiffs were not injured, they could not establish their
9 standing regardless of whether AT&T assisted the NSA with content surveillance.

10 **1. (U) Plaintiffs Cannot Establish Standing Because The State**
11 **Secrets Privilege Forecloses Litigation Over Whether They**
12 **Have Been Subject To Surveillance.**

13 (U) The issue of whether Plaintiffs can file a lawsuit alleging unlawful foreign
14 intelligence surveillance and then seek, in the first instance, to discover whether they have
15 actually been subject to such surveillance is not a new one. Courts have consistently refused to
16 recognize standing to challenge a Government surveillance program where the state secrets
17 privilege prevents a plaintiff from establishing, and the Government from refuting, that he was
18 actually subject to surveillance.

19 (U) In *Halkin I*, for example, a number of individuals and organizations claimed that they
20 were subject to unlawful surveillance by the NSA and CIA (among other agencies) due to their
21 opposition to the Vietnam War. *See* 598 F.2d at 3. The D.C. Circuit upheld an assertion of the
22 state secrets privilege regarding the identities of individuals subject to NSA surveillance,
23 rejecting the plaintiffs' argument that the privilege could not extend to the "mere fact of
24 interception," *id.* at 8, and despite significant public disclosures about the surveillance activities

1 at issue, *id.* at 10.²¹

2 (U) A similar state secrets assertion with respect to the identities of individuals subject to
3 CIA surveillance was upheld in *Halkin II*. See 690 F.2d at 991. There, as here, the plaintiffs
4 claimed that alleged NSA surveillance of their communications violated the Fourth Amendment.
5 Plaintiffs relied on the claim that their names were included on “watchlists” used to govern NSA
6 surveillance, arguing that this fact demonstrated a “substantial threat” that their communications
7 would be intercepted. See *id.* at 983-84, 997. The D.C. Circuit nevertheless affirmed dismissal
8 of the Fourth Amendment claim, “hold[ing] that appellants’ inability to adduce proof of actual
9 acquisition of their communications” rendered them “incapable of making the showing
10 necessary to establish their standing to seek relief.” *Id.* at 998. As here, plaintiffs “alleged, but
11 ultimately cannot show, a concrete injury” in light of the Government’s invocation of the state
12 secrets privilege. *Id.* at 999.²² The court thus found dismissal warranted, even though the
13 complaint alleged actual interception of plaintiffs’ communications, because the plaintiffs’
14 alleged injuries could be no more than speculative in the absence of their ability to prove that
15 such interception occurred.²³ *Id.* at 999, 1001; see also *Ellsberg*, 709 F.2d 51 (also holding that
16

17 ²¹ (U) As the court of appeals recognized, the “identification of the individuals or organizations
18 whose communications have or have not been acquired presents a reasonable danger that state
19 secrets would be revealed . . . [and] can be useful information to a sophisticated intelligence
analyst.” *Halkin I*, 598 F.2d at 9.

20 ²² (U) See *Halkin II*, 690 F.2d at 990 (“Without access to the facts about the identities of
21 particular plaintiffs who were subjected to CIA surveillance (or to NSA interception at the
22 instance of the CIA), direct injury in fact to any of the plaintiffs would not have been
23 susceptible of proof.”); *id.* at 987 (“Without access to documents identifying either the subjects
24 of . . . surveillance or the types of surveillance used against particular plaintiffs, the likelihood
of establishing injury in fact, causation by the defendants, violations of substantive
constitutional provisions, or the quantum of damages was clearly minimal.”).

25 ²³ (U) Because the CIA conceded that nine plaintiffs were subjected to certain types of
26 non-NSA surveillance, the D.C. Circuit held that those plaintiffs had demonstrated an

1 dismissal was warranted where a plaintiff could not, absent recourse to state secrets, establish
2 that he was actually subject to surveillance).

3 (U) In addition to foreclosing Plaintiffs' ability to prove standing for their constitutional
4 claims as in *Halkin*, the state secrets privilege would preclude Plaintiffs from establishing
5 standing as to their statutory claims. For example, FISA authorizes only an "aggrieved person"
6 to bring a civil action challenging the acquisition of communications contents. 50 U.S.C.
7 §§ 1801(f), 1810. To ensure that this term would be "coextensive [with], but no broader than,
8 those persons who have standing to raise claims under the Fourth Amendment with respect to
9 electronic surveillance," H.R. Rep. No. 95-1283, at 66 (1978), Congress defined "aggrieved
10 person" to mean one "whose communications or activities were *subject to* electronic
11 surveillance," 50 U.S.C. § 1801(k) (emphasis added). Litigants who cannot establish their status
12 as "aggrieved persons" therefore do "not have standing" under "any" of FISA's provisions. H.R.
13 Rep. No. 95-1283, at 89-90; cf. *United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987); see
14 also *Director, Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock*
15 *Co.*, 514 U.S. 122, 126 (1995) ("aggrieved" is a well-known term of art used "to designate those
16 who have standing").

17 (U) Title III similarly specifies that civil actions may be brought by a "person whose . . .
18 communication *is* intercepted, disclosed, or intentionally used." 18 U.S.C. § 2520(a) (emphasis
19 added). The Stored Communications Act likewise limits its civil remedies to "person[s]
20 aggrieved" under that statute, see 18 U.S.C. § 2707(a), and the only persons aggrieved by a
21 communication-service provider's "knowing[] divulge[nce]" of the "contents of a
22

23 injury-in-fact. See *Halkin II*, 690 F.2d at 1003. Nonetheless, the nine plaintiffs were precluded
24 from seeking injunctive and declaratory relief because they could not demonstrate the
25 likelihood of future injury or a live controversy in light of the fact that the CIA had terminated
26 the specific intelligence methods at issue. See *id.* at 1005-09.

1 communication” or of customer records, 18 U.S.C. § 2702(a), are those persons whose
2 communications or records were actually divulged. See 18 U.S.C. § 2711(1) (adopting
3 § 2510(11) definition of “aggrieved person” as one “who was a party to any intercepted . . .
4 communication” or “a person against whom the interception was directed”). Plaintiffs
5 additionally seek relief under 47 U.S.C. § 605, but this statute makes equally clear that only a
6 “person aggrieved” may challenge allegedly unlawful “divulge[nce] or publi[cation]” of the
7 contents of a communication, see 47 U.S.C. §§ 605(a), (e)(3)(A), and “only a party to a tapped
8 conversation may complain” of an alleged disclosure under § 605. See *United States ex rel.*
9 *Ross v. LaVallee*, 341 F.2d 823, 824 (2d Cir. 1965). Each of these provisions reflects the
10 fundamental point that only persons whose rights were injured by the actual interception or
11 disclosure of their own communications (or records) have standing. Put simply, to recover
12 damages, a plaintiff has to show that his or her rights were injured—and that cannot be done
13 here.

14 (U) With respect, we disagree with the Court’s statement in *Hepting* that allowing further
15 proceedings, such as discovery, before assessing the full impact of the state secrets privilege
16 would be consistent with *Halkin* and *Ellsberg*. See *Hepting*, 439 F. Supp. 2d at 994. In
17 *Halkin I*, the Government immediately moved to dismiss on state secrets grounds to protect facts
18 such as those at issue here—whether the plaintiffs were subject to surveillance and the methods
19 and techniques by which communications were intercepted. See 598 F.2d at 4-5. The
20 Government also opposed discovery requests, and responded only to court-propounded inquires
21 with a state secrets privilege assertion. See *id.* at 6. The district court upheld the claim of
22 privilege and dismissed the case as to one surveillance program (called MINARET), but denied
23 dismissal as to a separate program (called SHAMROCK) as to which some information had
24 been made public in Congressional hearings. See *id.* at 5. The Court of Appeals upheld the
25 privilege assertion and dismissal as to the MINARET program and *reversed* the district court
26

1 and upheld the privilege assertion as to the SHAMROCK program. *See* 598 F.2d at 8-11.

2 Specifically with respect to discovery, the Court of Appeals said:

3 In the case before us the acquisition of plaintiffs' communications is a fact vital
4 to their claim. No amount of ingenuity of counsel in putting questions on
5 discovery can outflank the government's objection that disclosure of this fact is
6 protected by privilege. Thus, in these special circumstances, we conclude that
7 affording additional discovery for the government to parry plaintiffs' requests
8 would be fruitless. *In camera* resolution of the state secrets question was
9 inevitable.

7 *Halkin I*, 598 F.2d at 6-7. As a result of this ruling, the claims against the NSA challenging the

8 alleged surveillance of the plaintiffs were dismissed on remand without any discovery. *See*

9 *Halkin II*, 690 F.2d at 984.

10 (U) A separate claim proceeded against the CIA for allegedly providing "watchlisting"
11 information to the NSA that was used to undertake surveillance. *See Halkin II*, 690 F.2d at 984.

12 While some document discovery occurred as to the defunct surveillance program at issue, which

13 had been the subject of a Congressional investigation, the CIA nonetheless successfully asserted

14 the state secrets privilege as to several facts, including whether any of the plaintiffs' names had

15 been submitted on any watchlists to the NSA. *See id.* at 985. The district court concluded that,

16 since the very fact of any interception was protected by NSA's state secrets assertion, the

17 plaintiffs would be unable to prove any liability on the part of CIA, and thus dismissed those

18 claims. The Court of Appeals affirmed, again upholding the state secrets privilege to bar

19 disclosure of the identities of individuals subject to surveillance, *see id.* at 988-89, 993 n.57, and

20 affirming dismissal for lack of standing, *see id.* at 997-1000. *See also id.* at 998 ("Since it is the

21 constitutionality of such interceptions that is the ultimate issue, the impossibility of proving that

22 interception of any [plaintiffs'] communications ever occurred renders the inquiry pointless from

23 the outset."). Thus, *Halkin II* likewise supports dismissal of claims challenging alleged

24 surveillance on state secrets grounds and without discovery. Whatever discovery that did occur

25 in *Halkin* was therefore irrelevant and wasteful, because the threshold fact of whether the

1 plaintiffs had been subject to surveillance could not be disclosed. Similarly, with respect to
2 those plaintiffs whom the government in *Ellsberg* had not admitted overhearing, the court found
3 that they lack an essential element of their proof of standing and that dismissal of their claims
4 was therefore proper. *See* 709 F.2d at 65.

5 (U) The same result is required here. Because the state secrets privilege precludes the
6 named Plaintiffs from demonstrating that they personally have been subject to surveillance
7 activities, litigation over Plaintiffs' standing is foreclosed. As explained in non-classified terms
8 by the DNI and NSA Director, the United States cannot confirm or deny whether any individual
9 is subject to alleged surveillance activities without causing potentially grave harm to the national
10 security, including by tending to reveal actual targets, sources, or methods. *See* Public
11 McConnell Decl. ¶ 14; Public Alexander Decl. ¶ 15. For example, if the NSA were to confirm
12 in this case and others that specific individuals are not targets of surveillance, but later refuse to
13 comment (as it would have to) in a case involving an actual target, a person could easily deduce
14 by comparing such responses that the person in the latter case is a target.

15 (U) The harm of revealing targets of foreign intelligence surveillance is obvious. If an
16 individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend
17 to alter his behavior to take new precautions against surveillance. *See id*; *see also Halkin I*, 598
18 F.2d at 9 (“the identity of particular individuals whose communications have been acquired can
19 be useful information to a sophisticated intelligence analyst”). Revealing who is not a target, in
20 turn, would indicate who has avoided surveillance and who may be a secure channel for
21 communication. *See* Public McConnell Decl. ¶ 14; Public Alexander Decl. ¶ 15. Such
22 information could lead a person, secure in the knowledge that he is not under surveillance, to
23 help a hostile foreign adversary convey information; alternatively, such a person may be
24 unwittingly utilized or even forced to convey information through a secure channel. *See id*.
25 Revealing which channels are free from surveillance and which are not would also reveal

1 sensitive intelligence methods and thereby could help any adversary evade detection. *See id.*
2 The consequences of identifying who is and is not subject to alleged surveillance activities may
3 vary depending on the circumstances. It is important to realize, however, that even a small piece
4 of information related to one individual Plaintiff could represent, to a sophisticated adversary, an
5 important “piece of the puzzle” of U.S. intelligence operations. *See Halkin I*, 598 F.2d at 8-9
6 (“[t]he significance of one item of information may frequently depend upon knowledge of many
7 other items of information” and “what may seem trivial to the uninformed, may appear of great
8 moment to one who has a broad view of the scene and may put the questioned item of
9 information in its proper context.”).

10 **2. (U) Plaintiffs Cannot Establish Standing On The**
11 **Basis Of A “Dragnet” Theory of Surveillance.**

12 (U) It bears specifically noting that Plaintiffs’ allegation of a “dragnet” of surveillance by
13 the Verizon Defendants—the interception of millions of domestic and international
14 communications made by ordinary Americans and transmitted by MCI and Verizon, *see, e.g., id.*
15 ¶¶ 3, 165—does not establish their standing. Even if that allegation were sufficient to avoid
16 dismissal through a standard Rule 12(b)(1) motion, facts concerning whether Plaintiffs have
17 been subject to any such dragnet of surveillance would obviously be essential to adjudicate their
18 standing for purposes of summary judgment.

19 (U) As an initial matter, the Plaintiffs have not even *alleged* that their communications
20 have been intercepted under the Terrorist Surveillance Program acknowledged by the President.
21 Indeed, the various complaints against the Verizon and MCI Defendants avoid any suggestion
22 that Plaintiffs might fall within the acknowledged and limited scope of the TSP.²⁴ Moreover, the
23 Court has already recognized that, in acknowledging that the TSP was a limited program aimed
24

25 ²⁴ (U) Accordingly, even if Plaintiffs did purport to challenge the TSP, they would lack
26 standing to do so on the face of their complaint.

1 at tracking international communications of members or agents of al Qaeda and affiliated
2 terrorist organizations, the Government denied that it was conducting the type of domestic
3 content dragnet that Plaintiffs allege. *See Hepting*, 439 F. Supp. 2d at 996. In order to prove
4 their standing for purposes of surviving the Government's summary judgment motion, therefore,
5 the named Plaintiffs are required to come forward with specific evidence rebutting the
6 Government's denial and establishing that they personally were subject to content surveillance.
7 But that cannot be done in light of the state secrets assertion. As previously explained, the DNI
8 has asserted the state secrets privilege over any information tending to confirm or deny whether
9 Plaintiffs were subject to surveillance, as well as program information about the TSP that
10 Plaintiffs likely would want disclosed to test, as an evidentiary matter, the limited scope of that
11 program. Because none of that information can be disclosed without revealing intelligence
12 targets, sources, and methods, Plaintiffs are not able to confirm or deny that they personally were
13 subject to surveillance (either under the TSP or their alleged domestic dragnet). Similarly, in
14 light of the privilege, Defendants are not able to offer evidence that would demonstrate any lack
15 of standing. Accordingly, summary judgment must be granted against the Plaintiffs.

16
17 [REDACTED TEXT]

18
19 **3. (U) Plaintiffs' Standing to Challenge Alleged Collection of**
20 **Communication Records Information Cannot be Adjudicated**
Without State Secrets.

21 (U) Plaintiffs' standing to challenge the alleged assistance of the Verizon Defendants
22 with an alleged program by the NSA to collect records about their communications, *see* Master
23 Verizon Compl. ¶ 226, cannot be adjudicated for the same reasons. The facts needed to
24 adjudicate standing would include not only *whether* such a program existed but, even if it did
25 exist and could be acknowledged by the Government, whether and how it may impact the
26

27 **Public Memorandum of the United States**
28 **in Support of Motion to Dismiss or for Summary**
Judgment, MDL No. 06-1791-VRW

1 Plaintiffs. Disclosure of such information would again reveal intelligence sources and methods,
2 confirming for our adversaries the nature and scope of what the Government does or does not do
3 and thereby enabling them to avoid detection.

4
5 [REDACTED TEXT]

6
7 **C. (U) The Disclosure of Facts Concerning the Alleged NSA Intelligence**
8 **Activities Is Required to Adjudicate Plaintiffs' Claims on the Merits.**

9 (U) As with the threshold issues of relationship and standing, Plaintiffs cannot prove the
10 merits of their case without establishing the existence of the alleged activities, that the Verizon
11 Defendants were involved in such activities, and that they are personally subject to such
12 activities—all of which is precluded by the state secrets privilege. And even assuming *arguendo*
13 that these threshold facts could be established (a possibility the Government disputes), the merits
14 of Plaintiffs' claims also could not be adjudicated without facts about the operation of any
15 alleged activity, including the precise nature of the activities, how they were conducted, why
16 they were conducted, when they were conducted and for how long, and the intelligence value of
17 the activities.

18 **1. (U) Plaintiffs' Claims as to Alleged Warrantless Content Surveillance**
19 **Cannot be Adjudicated Without Disclosing State Secrets.**

20 (U) This lawsuit commenced after media reports in December 2005 alleged that the NSA
21 was engaged in certain surveillance activities. *See* Master Verizon Compl. ¶¶ 138, 142; *Chulsky*
22 Compl. ¶¶ 18, 24; *Riordan* Compl. ¶ 20; *see also Hepting*, 439 F. Supp. 2d at 986. Plaintiffs cite
23 statements made at the time by the President, the Attorney General, and the Deputy Director of
24 National Intelligence acknowledging that the President had authorized the NSA to intercept the
25 content of one-end foreign communications where a party to the communication was reasonably
26 believed to be a member or agent of al Qaeda or an affiliated terrorist organization. For

1 example, the President has stated that the TSP was limited to surveillance of communications
2 and individuals associated with al Qaeda and did not involve the interception of purely domestic
3 calls in the United States. *See Hepting*, 439 F. Supp. 2d at 987 (taking judicial notice of
4 President's statement that the government's "international activities strictly target al Qaeda and
5 their know affiliates" and that "the government does not listen to domestic phone calls without
6 approval" and that the government is "not mining or trolling through the personal lives of
7 millions of Americans."); *see also* Master Verizon Compl. ¶ 139; *Chulsky* Compl. ¶ 25 (citing
8 statement by President on TSP). Attorney General Gonzales has likewise stated that the TSP
9 does not involve the interception of domestic to domestic calls within the United States. *See*
10 *Hepting*, 439 F. Supp. 2d at 987 (citing statements); *see also* Verizon Master Compl. ¶ 141;
11 *Chulsky* Compl. ¶ 26. Then-Deputy DNI, Gen. Michael Hayden, also stated regarding the scope
12 of the TSP:

13 The purpose of all this is not to collect reams of intelligence, but to detect and
14 prevent attacks. The intelligence community has neither the time, the resources,
15 nor the legal authority to read communications that aren't likely to protect us, and
16 the NSA has no interest in doing so. These are communications that we have
17 reason to believe are al Qaeda communications, a judgment made by intelligence
18 professionals. . . . This is targeted and focused. This is not about intercepting
19 conversations between people in the United States. This is hot pursuit of
20 communications entering or leaving America involving someone we believe is
21 associated with al Qaeda.

22 *See* Remarks of Gen. Michael V. Hayden, National Press Club, Jan. 23, 2006.

23 (U) Despite these plain denials that the TSP was a domestic content dragnet—denials
24 which the Court in *Hepting* acknowledged, *see* 439 F. Supp. 2d at 996—Plaintiffs allege without
25 any foundation, based on a newspaper article, that "the NSA intercepts *millions* of
26 communications made or received by people inside the United States" as part of a "massive
27 surveillance operation" for "data-mining" the "content" of millions of communications to find
28 those of particular interest. *See* Verizon Master Compl. ¶¶ 165, 167. They claim that the NSA
intercepts "*all* or a substantial number of the communications transmitted through [Verizon's]

1 key domestic telecommunication facilities, including direct access to streams of domestic,
2 international, and foreign telephone and electronic communications.” *Id.* ¶ 168. *See Hepting*,
3 439 F. Supp. 2d at 994 (“Plaintiffs allege a surveillance program of far greater scope than the
4 publicly disclosed ‘terrorist surveillance program.’”). In short, through their content surveillance
5 claim, Plaintiffs seek to prove whether the Government’s statements about the limited nature of
6 the TSP are true or whether Plaintiffs’ alleged dragnet actually exists and covered their own
7 communications. Plaintiffs thus allege that the NSA undertakes a secret content surveillance
8 program *other than and broader than* the TSP.

9 (U) The Court’s conclusion in *Hepting* that the Government’s acknowledgment of the
10 existence of the TSP has “opened the door for judicial inquiry” into the scope of any content
11 monitoring program undertaken by the NSA, *Hepting*, 433 F. Supp. 2d at 996, is unfounded in
12 our view (and is among the issues now on appeal). If such a disclosure did open the door to
13 further inquiry, state secrets would be needed to walk through it. The Court in *Hepting*
14 recognized that the Government “has disclosed the universe of possibilities in terms of *whose*
15 communications its monitors and *where* those communicating parties are located.” *See id.* As
16 the President stated, that universe involved the surveillance of communications (1) made by
17 parties reasonably believed to be members or agents of al Qaeda or affiliated terrorist
18 organizations, and (2) sent to or from the United States. But proving or disproving those two
19 facts as an evidentiary matter, in order to adjudicate Plaintiffs’ dragnet allegation, would require
20 the disclosure of TSP program information and perhaps other NSA surveillance methods and
21 activities, to show that the alleged dragnet of millions of domestic communications is not
22 occurring.²⁵ As set forth in the privilege assertions of DNI McConnell and NSA Director

23
24 ²⁵ (U) To the extent the Court in *Hepting* suggested that the proof needed to address whether or
25 not the alleged domestic content surveillance dragnet exists might be found in the scope of any
26 certification to a telecommunications carrier, *see id.* at 996-97, we again respectfully disagree.
That very relationship issue is among the matters subject to the Government’s privilege

27 **Public Memorandum of the United States**
28 **in Support of Motion to Dismiss or for Summary**
Judgment, MDL No. 06-1791-VRW

1 Alexander, those facts cannot be disclosed without causing exceptionally grave harm to national
2 security.

3
4 **[REDACTED TEXT]**

5
6 (U) The foregoing demonstrates that the TSP authorized by the President after 9/11 was
7 not directed at generalized domestic surveillance of the content of communications of millions
8 of Americans, as Plaintiffs allege. Moreover, to demonstrate that no *other* NSA program
9 involves the alleged domestic content dragnet, proof beyond the operation of the TSP would
10 have to be offered to demonstrate these facts (again, by having to prove a negative). But such
11 information also could not be disclosed without revealing sensitive NSA sources and methods to
12 our adversaries and thereby causing harm to the national security. Courts cannot allow litigants
13 “to force ‘groundless fishing expeditions’ upon them,” *Sterling*, 416 F.3d at 344, and a plaintiff
14 is not permitted to “embark on a fishing expedition in government waters on the basis of [its
15 own] speculation,” *Ellsberg v. Mitchell*, 807 F.2d 204, 207-08 (D.C. Cir. 1986) (Scalia, Circuit
16 Justice) (“*Ellsberg II*”). Litigation cannot proceed on claims where discovery of the actual facts
17 needed to prove or rebut allegations is barred by the state secrets privilege. *See Molerio v.*
18 *Federal Bureau of Investigation*, 749 F. 2d 815, 826 (D.C. Cir. 1984) (it would be “a mockery of
19 justice” to permit further proceedings where the actual facts are privileged).²⁶

20
21
22 assertion, and to put that matter at risk in order to demonstrate that an allegation *already denied*
23 *by the Government* is false, would be unfounded.

24 ²⁶ (U) Because Plaintiffs neither allege that the TSP applies to them nor challenge that
25 program, the lawfulness of the TSP is not at issue here. Even if they did challenge the TSP,
26 however, classified details about the program, as described in the *In Camera* Alexander
Declaration, would be needed to adjudicate its lawfulness.

27 Public Memorandum of the United States
in Support of Motion to Dismiss or for Summary
28 Judgment, MDL No. 06-1791-VRW

1 2. **(U) Plaintiffs' Challenge to Alleged Communication Records**
2 **Collection Cannot be Adjudicated Without Disclosing State Secrets.**

3 (U) Plaintiffs' challenge to the alleged collection of communication records likewise
4 cannot be adjudicated without disclosing state secrets. *See Terkel*, 441 F. Supp. 2d at 919-20
5 (holding that disclosure of whether or not AT&T has assisted the government's intelligence
6 activities by providing large quantities of telephone records "would adversely affect our national
7 security" and therefore is "barred by the state secrets privilege"). The Court in *Hepting* correctly
8 found that information confirming or denying an alleged communication records program should
9 remain protected from disclosure. *See* 439 F. Supp. 2d at 997-98. Indeed, the Court recognized
10 the potential harm of confirming or denying such allegations, and it also appropriately held that
11 it is not in a position to second-guess the judgment of the DNI and NSA Director regarding such
12 harm.

13 (U) At the same time, we respectfully believe that the Court's decision not to dismiss the
14 records claim—a decision based on the "conceivable" possibility that deliberate or even
15 accidental disclosures about the records allegations could be made in the future—was erroneous.
16 *See id.* at 997. First, the Government has consistently maintained that the records allegations
17 could not be confirmed or denied without harming national security, and it is inappropriate for
18 the Court to keep the claims open on the chance that such harmful disclosures might be made,
19 even accidentally, at some undetermined future date. Moreover, the suggestion that public
20 disclosures of private entities might waive the state secrets privilege is incorrect. As outlined
21 above, whether information may be protected under the state secrets privilege turns on whether
22 the Government has reasonably shown that harm would flow from disclosure of that
23 information. Unless an authorized official of the United States Government formally confirms
24 or denies the existence of an alleged activity, any other public statement or disclosure,
25 particularly "accidental" ones, cannot trump the Government's assertion of privilege. For these
26 reasons, the Court in *Terkel* correctly dismissed a case alleging that AT&T participated in an

1 illegal record program. *See* 441 F. Supp. 2d at 916, 919-20. To the extent this Court has any
2 remaining doubts about whether the records claims should be dismissed here, we wish to
3 emphasize the following.

4
5 **[REDACTED TEXT]**

6
7 (U) Assuming, *arguendo*, that the alleged records program did exist and was confirmed
8 by the Government, numerous facts about the operation of any such program would be needed to
9 determine its lawfulness, including how the activity proceeds, whose information may be
10 collected, what may be done with the information, and why the information may be
11 collected—all of which, if such activity occurred, would reveal intelligence sources and methods
12 to our adversaries. For example, civil liability provisions of the Stored Communications Act
13 require proof of actual damages by the plaintiff, *see* 18 U.S.C. § 2707(c), and that would require
14 showing that an action was taken against an individual plaintiff that caused that person actual
15 damages. Similarly, the Supreme Court has held that an individual has no Fourth Amendment
16 protected legitimate expectation of privacy regarding the numbers dialed on a telephone, *see*
17 *Smith v. Maryland*, 442 U.S. 735, 742 (1979), and this issue could not be adjudicated without
18 describing the extent to which the NSA, if it does at all, collects data in which there is an
19 expectation of privacy. Similarly, the need for any such activity would be relevant evidence in
20 deciding the lawfulness of such a program, *see Vernonia Sch. Dist. v. Action*, 515 U.S. 646, 653
21 (1995) (there are circumstances when special needs, beyond the normal need for law
22 enforcement, make the warrant and probable cause requirement impracticable).²⁷ Finally, the

23
24 ²⁷ (U) Similarly, the Stored Communications Act provides that a telecommunication carrier
25 may divulge customer records “to a governmental entity, if the provider reasonably believes
26 that an emergency involving immediate danger or death or serious physical injury to any person
justifies disclosure of the information.” 18 U.S.C. § 2702(c)(4).

27 **Public Memorandum of the United States**
in Support of Motion to Dismiss or for Summary
28 **Judgment, MDL No. 06-1791-VRW**

1 efficacy of a challenged activity is another factor in assessing its lawfulness. *See Vernonia*, 515
2 U.S. at 663. Thus, even assuming purely for the sake of argument that one could show that a
3 particular activity is occurring, the evidence needed to adjudicate a challenge on the merits
4 implicates host of different facts, all of which implicate the existence, scope, and nature of
5 alleged intelligence sources and methods.

6 [REDACTED TEXT]

7
8 **IV. (U) STATUTORY PRIVILEGE CLAIMS HAVE ALSO BEEN PROPERLY
9 RAISED IN THIS CASE.**

10 (U) Two statutory protections also apply to the intelligence-related information, sources
11 and methods at issue in this case, and both have been properly invoked here as well. First,
12 Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64,
13 codified at 50 U.S.C. § 402 note, provides:

14 [N]othing in this Act or any other law . . . shall be construed to require the
15 disclosure of the organization or any function of the National Security Agency,
16 of any information with respect to the activities thereof, or of the names, titles,
17 salaries, or number of persons employed by such agency.

18 *Id.* Section 6 reflects a “congressional judgment that in order to preserve national security,
19 information elucidating the subjects specified ought to be safe from forced exposure.” *The*
20 *Founding Church of Scientology of Washington, D.C., Inc. v. Nat’l Security Agency*, 610 F.2d
21 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat’l Security Agency*, 608 F.2d 1381, 1389 (D.C.
22 Cir. 1979). In enacting Section 6, Congress was “fully aware of the ‘unique and sensitive’
23 activities of the [NSA] which require ‘extreme security measures.’” *Hayden*, 608 F.2d at 1390
24 (citing legislative history). Thus, “[t]he protection afforded by Section 6 is, by its very terms,
25 absolute. If a document is covered by Section 6, NSA is entitled to withhold it” *Linder v.*
26 *Nat’l Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996).

1 (U) The second applicable statute is Section 102A(i)(1) of the Intelligence Reform and
2 Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004),
3 codified at 50 U.S.C. § 403-1(i)(1). This statute requires the Director of National Intelligence to
4 protect intelligence sources and methods from unauthorized disclosure. The authority to protect
5 intelligence sources and methods from disclosure is rooted in the “practical necessities of
6 modern intelligence gathering,” *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990), and has
7 been described by the Supreme Court as both “sweeping,” *CIA v. Sims*, 471 U.S. at 169, and
8 “wideranging,” *Snepp v. United States*, 444 U.S. 507, 509 (1980). Sources and methods
9 constitute “the heart of all intelligence operations,” *Sims*, 471 U.S. at 167, and “[i]t is the
10 responsibility of the [intelligence community], not that of the judiciary to weigh the variety of
11 complex and subtle factors in determining whether disclosure of information may lead to an
12 unacceptable risk of compromising the . . . intelligence-gathering process.” *Id.* at 180.

13 (U) These statutory privileges have been properly asserted as to any intelligence-related
14 information, sources and methods implicated by Plaintiffs’ claims, and the information covered
15 by these privilege claims are at least co-extensive with the assertion of the state secrets privilege
16 by the DNI. *See* Public McConnell Decl. ¶ 10; Public Alexander Decl. ¶ 12. Moreover, these
17 privileges reinforce the conclusion that the state secrets privilege requires dismissal here, and
18 provide an additional, independent basis for that conclusion. The fact that intelligence sources
19 and methods, as well as information concerning NSA activities, are subject to express statutory
20 prohibitions on disclosure underscores that the need to protect such information does not reflect
21 solely a policy judgment by the Executive Branch, but the judgment of Congress as well.

22 (U) Since the Court’s decision in *Hepting*, Section 6 of the National Security Act has
23 been applied in a FOIA context to information concerning the Terrorist Surveillance Program.
24 *See People for the American Way Foundation v. National Security Agency/Central Security*
25 *Service*, 462 F. Supp. 2d 21 (D.D.C. 2006). In *PAFW*, the court applied Section 6 to preclude
26

1 disclosure under FOIA of several categories of information related to the TSP, including the
2 number of individuals subject to surveillance under the program, the number of communications
3 intercepted, the identity of individuals targeted and, in particular, information that would
4 confirm or deny whether the plaintiffs in that case had been subject to TSP surveillance—the
5 very kind of information at issue in this case. *See id.* at 29. The court agreed that the NSA had
6 put forward a rational explanation as to why this information should be upheld under Section 6,
7 including that it would reveal information about NSA’s success or lack of success under the
8 TSP, as well as information about the U.S. intelligence communities capabilities, priorities, and
9 activities. *See id.* The court also agreed that confirmation by NSA that a particular person’s
10 activities are not of a foreign intelligence interest or that NSA is unsuccessful in collecting
11 foreign intelligence information on their activities “would allow our adversaries to accumulate
12 information and draw conclusions about NSA’s technical capabilities, sources, and methods.”
13 *See id.*

14 (U) The court in *PFAW* also held that Section 6 of the National Security Act does not
15 require NSA to demonstrate what harm might result from disclosure of its activities, since
16 “Congress has already, in enacting the statute, decided that disclosure of NSA activities is
17 potential harmful.” *See PFAW*, 462 F. Supp. 2d at 30 (quoting *Hayden*, 608 F.2d at 1390).
18 Finally, the court in *PFAW* rejected the contention that, because the legality of the TSP is at
19 issue, Section 6 does not apply to protect information about NSA activities. The court held:

20 Whether the TSP, one of the NSA’s many SIGINT programs involving the
21 collection of electronic communications, is ultimately determined to be unlawful,
22 its potential illegality cannot be used to evade the “unequivocal[]” language of
Section 6 which “prohibit[s] the disclosure of information relating to the NSA’s
functions and activities . . .”

23 *PFAW*, 462 F. Supp. 2d at 31 (quoting *Linder*, 94 F.3d at 696).²⁸

24
25 ²⁸ (U) The Court in *PFAW* also agreed that the TSP information at issue in that case was
26 protected by the DNI’s statutory privilege under 50 U.S.C. 403-1(i)(1). *See* 462 F. Supp. 2d at

27 **Public Memorandum of the United States**
in Support of Motion to Dismiss or for Summary
28 **Judgment, MDL No. 06-1791-VRW**

1 (U) The Court in *Hepting* essentially disregarded the Government’s statutory privilege
2 assertions. The Court observed that “[n]either of these provisions by their terms requires the
3 court to dismiss this action . . .” *Hepting*, 439 F. Supp. 2d at 998. That is true, but beside the
4 point. A statutory privilege bars the disclosure of information; the consequences of that
5 Congressional mandate are then determined in whatever proceeding the information is sought.
6 Here, the information that Congress has barred from disclosure is central to adjudication of the
7 case from the outset. As with the state secrets privilege, the Court’s decision in *Hepting* to
8 “determine step-by-step whether the privilege will prevent plaintiffs from discovering particular
9 evidence,” amounted to a non-decision on the substance of the statutory and state secrets
10 privilege assertions. If, as is the case here, certain information is subject to the privilege, and if
11 that information must be excluded under an executive privilege and by statutory law, and if as a
12 result the case cannot proceed without that evidence, then there are no grounds for further
13 proceedings.

14 [REDACTED TEXT]

15 (U) CONCLUSION

16 (U) For the foregoing reasons, the Court should:

- 17 1. Uphold the United States’ assertion of the military and state secrets privilege and
18 exclude from this case the information identified in the Declarations of J. Michael McConnell,
19 Director of National Intelligence, and Lt. Gen. Keith B. Alexander, Director of the National
20 Security Agency; and
- 21 2. Dismiss this action or enter summary judgment for the United States because
22 adjudication of Plaintiffs’ claims requires the disclosure of state secrets and, thus, risks
23 exceptionally grave harm to the national security of the United States.
24

25 _____
26 31 n.8.

27 Public Memorandum of the United States
28 in Support of Motion to Dismiss or for Summary
Judgment, MDL No. 06-1791-VRW

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

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

CARL J. NICHOLS
Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

s/ Andrew H. Tannenbaum
ANDREW H. TANNENBAUM
Trial Attorney
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202

Attorneys for United States of America

DATED: April 20, 2007

Public Memorandum of the United States
in Support of Motion to Dismiss or for Summary
Judgment, MDL No. 06-1791-VRW