

No. 06-17137

(Consolidated with Nos. 06-17132, 06-36083)

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

TASH HEPTING, et al., Plaintiffs - Appellees,

v.

AT&T CORP., et al., Defendants, and

UNITED STATES OF AMERICA, Intervenor - Appellant.

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

REPLY BRIEF FOR THE UNITED STATES

PAUL D. CLEMENT
Solicitor General

PETER D. KEISLER
Assistant Attorney General

GREGORY G. GARRE
Deputy Solicitor General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG

DARYL JOSEFFER
Assistant to the Solicitor
General

Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
INTRODUCTION	1
I. THIS CASE MUST BE DISMISSED BECAUSE ITS “VERY SUBJECT MATTER” IS A STATE SECRET	4
II. THIS CASE MUST BE DISMISSED BECAUSE NEITHER STANDING NOR THE MERITS MAY BE LITIGATED WITHOUT DISCLOSING STATE SECRETS	6
III. CONGRESS HAS NOT ABROGATED THE STATE SECRETS PRIVILEGE	21
CONCLUSION	29
ADDENDUM	
CERTIFICATE OF COMPLIANCE	
CERTIFICATE OF SERVICE	

TABLE OF AUTHORITIES

Cases:

<i>ACLU Found. v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991)	23, 26, 27
<i>Afshar v. Department of State</i> , 702 F.2d 1125 (D.C. Cir. 1983)	14
<i>Armstrong v. Bush</i> , 924 F.2d 282 (D.C. Cir. 1991)	22
<i>Black v. United States</i> , 62 F.3d 1115 (8th Cir. 1995)	15
<i>California v. United States</i> , 215 F.3d 1005 (9th Cir. 2000)	22
<i>Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council</i> , 485 U.S. 568 (1988)	21
<i>El-Masri v. United States</i> , 479 F.3d 296 (4th Cir. 2007)	12, 15, 21, 29
<i>Fitzgerald v. Penthouse Int’l Ltd.</i> , 776 F.2d 1236 (4th Cir. 1985)	14
<i>In re Grand Jury Investigation</i> , 437 F.3d 855 (9th Cir. 2006)	26
<i>Halkin v. Helms (“Halkin IP”)</i> , 690 F.2d 977 (D.C. Cir. 1982)	17, 28
<i>Kasza v. Browner</i> , 133 F.3d 1159 (9th Cir. 1998)	2, 6, 8, 12, 15, 22, 28

<i>Linder v. National Security Agency</i> , 94 F.3d 693 (D.C. Cir. 1996)	22
<i>Norfolk Redevelopment & Housing Auth. v. Chesapeake & Potomac Tel. Co.</i> , 464 U.S. 30 (1983)	22
<i>Tenet v. Doe</i> , 544 U.S. 1 (2005)	2, 4, 5, 12
<i>Terkel v. AT&T Corp.</i> , 441 F. Supp. 2d 899 (N.D. Ill. 2006)	14
<i>Totten v. United States</i> , 92 U.S. 105 (1875)	2, 4, 5, 12
<i>United States v. Nixon</i> , 418 U.S. 683 (1974)	21
<i>United States v. Reynolds</i> , 345 U.S. 1 (1953)	28
<i>United States v. Tobias</i> , 836 F.2d 449 (9th Cir. 1988)	26
<i>Weinberger v. Catholic Action of Hawaii</i> , 454 U.S. 139 (1981)	5, 15
<i>Zuckerbraun v. General Dynamics Corp.</i> , 935 F.2d 544 (2d Cir. 1991)	15

U.S. Constitution:

Article II	21
Section 2	28
Article III	16

Statutes:

Foreign Intelligence Surveillance Act of 1978 (“FISA”), as amended, 50 U.S.C. 1801-1871	
50 U.S.C. 1801(g)	28
50 U.S.C. 1801(k)	24
50 U.S.C. 1805(a)	25
50 U.S.C. 1806	23
50 U.S.C. 1806(c)	23, 25
50 U.S.C. 1806(d)	23
50 U.S.C. 1806(e)	23
50 U.S.C. 1806(f)	21, 23, 24, 25, 26, 27, 28
50 U.S.C. 1806(g)	24
50 U.S.C. 1806(j)	25
National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (1959)	22
Section 6 (50 U.S.C. § 402 note)	22
18 U.S.C. 3504	26
18 U.S.C. 3504(a)(1)	26
18 U.S.C. 3504(b)	26
28 U.S.C. 514	28
28 U.S.C. 516	28
28 U.S.C. 519	28

Legislative Materials:

H.R. Conf. Rep. No. 95-1720 (1978)	27
S. Rep. No. 95-604 (1977)	24
S. Rep. No. 95-701 (1978)	24, 26, 27

Miscellaneous:

Appellants' Brief in *Kasza v. Browner* (9th Cir. 1998),
1996 WL 33418896 12

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

No. 06-17137

**TASH HEPTING, et al.,
Plaintiffs - Appellees,**

v.

**AT&T CORP., et al.,
Defendants,**

and

**UNITED STATES OF AMERICA,
Intervenor - Appellant.**

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

REPLY BRIEF FOR THE UNITED STATES

INTRODUCTION

Plaintiffs concede (Br. 82) that they are not challenging surveillance that was conducted under the now-defunct Terrorist Surveillance Program (“TSP”), and they largely abandon their challenge to the alleged “communications records” program. Instead, plaintiffs now focus their challenge on their allegations that the Government is undertaking a secret program of “indiscriminately” intercepting the contents of

“telephone and Internet communications of millions of [individuals]” pursuant to a “surveillance dragnet,” and that AT&T is participating in that program. Br. 1, 24. The Government has never acknowledged the existence of any such “dragnet” program (or AT&T’s involvement in any such program). To the contrary, the Government has denied the existence of such a program and asserted the state secrets privilege over the means, sources, and methods of the Government’s foreign surveillance activities, explaining that disclosing such information would severely undermine the Nation’s intelligence capabilities. This action is accordingly tailor-made for applying the state secrets privilege.

As explained in the Government’s opening brief, this action must be dismissed under the state secrets doctrine both because its very subject matter is a state secret, and because plaintiffs’ standing and the merits of their claims cannot be litigated without disclosing state secrets. As to the first ground for dismissal, plaintiffs concede (Br. 24) that the “subject matter of this action” is whether AT&T participated in the alleged “dragnet” program. Because that “subject matter” is itself a state secret, dismissal is compelled under this Court’s decision in *Kasza v. Browner*, 133 F.3d 1159 (9th Cir. 1998), and the Supreme Court’s decisions in *Totten v. United States*, 92 U.S. 105 (1875), and *Tenet v. Doe*, 544 U.S. 1 (2005). Plaintiffs argue that *Totten* and *Tenet* bar litigation over covert espionage relationships only where suit is brought *by the claimed spy*. But these precedents preclude litigation whenever success

depends upon the existence of an alleged secret espionage relationship with the Government. That rationale compels dismissal here.

As to the second ground for dismissal, plaintiffs argue that the state secrets privilege is inapplicable because they can assertedly establish on the public record that AT&T has collaborated with the Government with respect to their alleged surveillance program. But any attempt by plaintiffs to establish that a content “dragnet” exists, or by the Government to prove that it does not, would require disclosure of privileged information regarding what, if any, surveillance activities the Government is or has been conducting, and what role, if any, AT&T is or has been playing in any such activities. The same goes for any effort by plaintiffs to establish their standing by showing that their communications were intercepted under the alleged “dragnet” program. This case therefore presents a classic situation in which the state secrets privilege requires dismissal.

Nor can plaintiffs avoid this fatal justiciability flaw by relying on unconfirmed speculation in the media and in the declarations of Mark Klein and Scott Marcus. The state secrets privilege cannot be vitiated by the speculation of individuals lacking knowledge of secret Government activities. Moreover, contrary to plaintiffs’ contention, the Government does not “waive” the state secrets privilege by failing to seek to “suppress” the uninformed speculation of such individuals. The pertinent

point is that the Government has never acknowledged the alleged “dragnet” program, and, indeed, has denied it exists.

Finally, there is no merit to plaintiffs’ argument that Congress, in enacting the FISA, implicitly abrogated the constitutionally-based state secrets privilege in the electronic surveillance context. This contention finds no support in statutory text, legislative history, or judicial precedent, and the district court properly declined to accept it. The state secrets privilege therefore requires dismissal.

I. THIS CASE MUST BE DISMISSED BECAUSE ITS “VERY SUBJECT MATTER” IS A STATE SECRET.

Plaintiffs acknowledge that “the subject matter of this action is whether AT&T participated in [the alleged secret] program of electronic surveillance.” Br. 24. In addition, plaintiffs acknowledge that, to establish their claims, they must prove not only that AT&T intercepted communications information, but that “AT&T acquired it for and disclosed it to the Government.” Br. 61. The very subject matter of plaintiffs’ claims is thus itself a state secret, as explained by the Government’s public and classified declarations. Moreover, plaintiffs’ claims rest upon an alleged secret espionage relationship between the Government and AT&T that cannot be adjudicated under *Totten* and *Tenet*. See Gov. Br. 16-24.

Plaintiffs argue that the precedential scope of *Totten* and *Tenet* is limited to contract actions brought by spies. Br. 46-48. That argument is directly contradicted

by *Tenet*'s reliance on *Weinberger v. Catholic Action of Hawaii*, 454 U.S. 139 (1981), and by the reasoning of *Totten* itself. *Totten*'s holding reflects the “general principle that public policy forbids the maintenance of *any suit* in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential.” 92 U.S. at 107 (emphasis added). The claim in *Totten* thus could not be maintained because litigation over a secret espionage relationship would expose a clandestine function, the “manner of its discharge,” and other details “to the *serious detriment to the public.*” *Id.* at 106-07 (emphasis added).

In *Tenet*, the Supreme Court accordingly rejected the notion that “*Totten* developed merely a contract rule” for espionage agreements. See 544 U.S. at 8. To the contrary, *Totten* applies whenever litigation “success depends upon the existence of [an alleged] secret espionage relationship with the Government” (*ibid.*), because its “core concern [is] preventing the *existence* of the [purported] relationship with the Government from being revealed.” *Id.* at 10 (emphasis added). Application of that principle requires dismissal here because—as plaintiffs acknowledge (Br. 24, 61)—their litigation success depends on establishing the existence of a secret espionage relationship between AT&T and the Government.

II. THIS CASE MUST BE DISMISSED BECAUSE NEITHER STANDING NOR THE MERITS MAY BE LITIGATED WITHOUT DISCLOSING STATE SECRETS.

A. As this Court explained in *Kasza*, litigation must be dismissed when the “very subject matter” of a case is a state secret, the plaintiff cannot prove a *prima facie* case with nonprivileged evidence, or the privilege “deprives the defendant of information that would otherwise give the defendant a valid defense to the claim.” 133 F.3d at 1166. Here, the Government invoked the state secrets privilege over the means, methods, and targets of surveillance, including whether AT&T participated in such surveillance. Gov. Br. 7. The Director of National Intelligence explained that those matters are quintessential state secrets. ER 58-59; see ER 64. The Government’s invocation of the privilege renders it impossible for plaintiffs to prove either standing or the merits of their claims, and for AT&T to defend itself against plaintiffs’ allegations, because doing so would require (at a minimum) inquiring into (1) the existence of the alleged “dragnet” program, (2) AT&T’s participation in any such program, and (3) whether plaintiffs’ communications were intercepted by AT&T under such a program.

The state secrets privilege applies even more clearly because plaintiffs are now challenging only an alleged “indiscriminate[]” “dragnet” program intercepting the content of communications of millions of Americans (Br. 1, 82), which the Government has never acknowledged, and has indeed *denied*. As the district court

correctly recognized, the United States “denies listening in without a warrant on any purely domestic communications,” or on “communications in which neither party has a connection to al Qaeda or a related terrorist organization.” ER 327-28. The President himself emphasized that the “government does *not* listen to domestic phone calls without court approval,” and is “*not* mining or trolling through the personal lives of millions of innocent Americans.” ER 320 (emphasis added).

Plaintiffs respond that they have produced “detailed and unrebutted evidence” (Br. 1), on the *public* record, “proving that AT&T has been collaborating with the NSA in the surveillance of the domestic communications of millions of Americans,” (*id.* at 5), and that, therefore, they can “prove their case without resort to state secrets.” See Br. 18 36, 37, 68. As discussed below, however, the “evidence” to which plaintiffs refer consists of *speculation* by the media and plaintiffs’ own witnesses, who lack any first-hand knowledge of the Government’s surveillance efforts. Plaintiffs have not remotely shown that they could prove either standing or the merits of their claims without state secrets. Even if they attempted to do so, the Government and AT&T could not fairly defend themselves because of state secrets.

Moreover, the only reason plaintiffs can claim to have adduced “unrebutted” evidence is that the subject matter of this case involves state secrets. Any attempt by the Government (or AT&T) to prove its “dragnet” denial would necessarily depend on state secrets. Even apart from the relationship issue, the process of “proving a

negative”—that plaintiffs’ unsubstantiated content “dragnet” allegations are false—could not be resolved without disclosing what activities the NSA does and does not conduct. That process would implicate highly classified and sensitive facts essential to the efficacy of ongoing foreign intelligence operations. A plaintiff cannot vitiate the state secrets privilege simply by assuming that his proffered evidence, and the deductions one might draw from it, are correct. That would permit any individual to destroy critical state secrets simply by going to court with speculation.

Nor does the fact that the Government has denied the alleged “dragnet” open the door for plaintiffs to litigate the “veracity of the [G]overnment’s denial.” See *Kasza*, 133 F.3d at 1172. A case involving state secrets “is not a normal case,” and, in this context, litigants are “denied the tools normally available for testing credibility.” *Ibid.* The state secrets doctrine accounts for a plaintiff’s inability to “challeng[e] the credibility of the [G]overnment’s representations” by permitting the Judiciary to “satisfy itself of the credibility of the [Executive’s] public declarations in the course of its *in camera* review” of classified declarations supporting the privilege. *Ibid.* While such materials will rarely (if ever) present the Government’s full defense of a case, a court’s “narrow” review of those materials can both give ““utmost deference”” to the Executive’s representations (*id.* at 1166), while providing a circumscribed means for ensuring that the Government’s denials are facially credible. Review of the classified declarations here readily satisfies this inquiry.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 10]

B. Plaintiffs' reliance on the Klein and Marcus declarations and other speculation about the Government's surveillance activities—reliance disavowed by the district court (ER 322)—is unavailing. See, e.g., Br. 5-10, 75-76. These statements are not competent evidence and are inconclusive as to whether they relate to the alleged surveillance activities. Most importantly, they are not statements by the Executive. Public speculation and inferences drawn from it are often inaccurate. The Nation's compelling interest in protecting classified intelligence matters from disclosure is not reduced, much less thwarted, by such speculation.

Plaintiffs' reliance on the Klein and Marcus declarations is misplaced. Klein, a former AT&T technician, explained that, while still with AT&T, a site manager *told him* that another AT&T employee, "cleared and approved" by NSA, was working on a "special job" installing equipment in a limited-access room at an AT&T facility. AER 67-68. Klein stated that, while he himself did not have any relevant clearance, "to [his] knowledge, only employees cleared by the NSA" were allowed in that room. AER 69, 87. He identified no source or basis for that "knowledge." Klein added that he reviewed documents instructing technicians on how to connect AT&T's WorldNet Internet fiber-optic circuits to the limited-access room. AER 70. From this hearsay and other tidbits, Klein surmised that the content of all Internet communications going across certain circuits were "transferred" into the room. AER 71; see *id.* at 88-89.

For his part, Marcus, an engineer, addressed “the implications of” the Klein declaration. AER 78. Without any personal knowledge of AT&T’s operations, and based solely on a document review, Marcus concluded that “AT&T has constructed an extensive—and expensive—collection of infrastructure that collectively has all the *capability* necessary to conduct large scale covert gathering of IP-based communications information.” AER 85 (emphasis added). Based on the documents he reviewed, Marcus speculated that, “*if* the government is in fact in communication with this infrastructure, [it] *would have* the capacity to monitor both domestic and international communications of persons in the United States.” *Ibid.*

Neither of these declarations undercuts the Government’s assertion of the state secrets privilege. Klein acknowledged that he was not authorized to enter the alleged secret room; he did not claim to know what was in the room; and, although he speculated as to NSA involvement with the room, he made no claim that (and had no way of knowing whether) NSA was actually utilizing the room in any particular way, much less that it was using it for surveillance, let alone *domestic* surveillance. See AER 66-72; see also SER 1-7. Marcus’s declaration, which was based only on a review of Klein’s submission and selected newspaper stories, is even more speculative. As noted, Marcus had no first-hand knowledge of the facilities, and was able to conclude, at most, that “*if* the government is in fact in communication with th[e] infrastructure” described by Klein, it “would have the *capacity* to monitor both

domestic and international communications of persons in the United States.” AER 85 (emphasis added). As the district court recognized, such speculation (based on multiple layers of hearsay) by persons with no direct knowledge of the facts cannot override the Government’s state secrets assertion. See ER 322.

Furthermore, even if Klein and Marcus had direct knowledge of relevant facts, the result would be the same. The alleged spies in *Tenet* and *Totten* purported to have direct knowledge of facts supporting their claims, just as the plaintiffs in *Kasza* “who worked at [the] classified operating location” at issue there proffered evidence based on first-hand knowledge and unclassified materials. Compare, e.g., *Kasza*, 133 F.3d at 1162-63, 1171-72, with *Kasza* Appellants’ Brief, 1996 WL 33418896, at *18-*24. Regardless of such knowledge and evidence, this Court held that the need to litigate state secrets in *Kasza* mandated dismissal. The need for dismissal here follows *a fortiori* from *Kasza*, given that plaintiffs’ declarations are based on the speculation of individuals who lack first-hand knowledge of the alleged secret espionage relationship. See also *El-Masri v. United States*, 479 F.3d 296 (4th Cir. 2007).

Plaintiffs suggest (see, e.g., Br. 3-4, 15-16, 18, 38) that the Government “conceded” (Br. 4, 15, 36, 37, 39) away the applicability of the privilege when Assistant Attorney General Keisler explained in district court that “[w]e have not asserted any privilege over the information that is in the Klein or Marcus declarations.” AER 189. That contention is absurd. Mr. Keisler simply explained

that “Klein and Marcus never had access to any of the relevant classified information here, and with all [due] respect to them, through no fault or failure of their own, they don’t know anything.” *Ibid.* Because they “don’t know anything,” their public ruminations about the Government’s surveillance activities are no more subject to the assertion of the state secrets privilege than other speculation.

Plaintiffs’ claim that the Government “waived” the state secrets privilege because it did not seek to “suppress” the Klein and Marcus declarations (see Br. 15, 38, 65) is likewise incorrect. It is not unusual (as here) for persons lacking access to the facts to speculate regarding alleged confidential Government activity. Indeed, such speculation is commonly reflected in news reports. The Government typically does not attempt to “suppress” such speculation, and thereby does not “waive” the public’s right to protect state secrets. Under plaintiffs’ view, any time someone publicly speculated about a matter touching on state secrets, the Government would have to seek to “suppress” the statement—regardless of whether the statement had any validity, or was entirely false—or else risk “waiving” the state secrets privilege as to any underlying secrets. There is no precedent or justification for such a bizarre “waiver” rule.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 14]

Plaintiffs similarly err in arguing that media reports speculating about NSA activities can effectively defeat the state secrets privilege. See Br. 10-11. As the district court properly concluded, media speculation does not undo the privilege; otherwise, individuals could force disclosure of highly classified secrets merely by speculating about them in public. See ER 321-22; *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 913-15 (N.D. Ill. 2006). Nor is this analysis altered because some of the cited stories feature statements attributed to Members of Congress—statements that appear to refer to communications *records*, rather than the alleged content “dragnet” that plaintiffs challenge. See Br. 10-11. The individual statements of legislators do not speak for the Executive Branch, and do not override the President’s constitutionally-based power to protect national security information. See generally *Fitzgerald v. Penthouse Int’l Ltd.*, 776 F.2d 1236, 1242-43 (4th Cir. 1985); *Afshar v. Department of State*, 702 F.2d 1125, 1130-31 (D.C. Cir. 1983).^{1/}

C.1. Plaintiffs assert that dismissal at this stage is appropriate only if the very subject matter of the action is a state secret. As discussed, the very subject matter is

^{1/} The district court’s treatment of plaintiffs’ communications records claim underscores its mistaken approach to this case. The court agreed that there could be no discovery on this point because no such activities had been confirmed or denied, but it nevertheless refused to dismiss the claim, reasoning that further intentional or inadvertent disclosures “might make this program’s existence or non-existence no longer a secret.” ER 329. Our opening brief demonstrated (at 25-26) the unsustainability of this analysis, and plaintiffs make no serious attempt to defend it.

a state secret, and dismissal is therefore appropriate for that reason alone. In any event, plaintiffs are incorrect in arguing that dismissal is not otherwise required if the Court concludes that they cannot litigate standing or the merits.

Dismissal is required when further litigation would “inevitably lead to the disclosure of matters which the law itself regards as confidential.” *Weinberger*, 454 U.S. at 147. There is no reason to jeopardize national security by continuing with litigation once it is apparent that state secrets are needed to adjudicate the case. Thus, contrary to plaintiffs’ contention that dismissal is rarely appropriate in state secrets cases, numerous courts have recognized that dismissal is required where, as here, allegations cannot be “fairly litigated” without “threatening the disclosure of * * * state secrets.” See *El-Masri*, 479 F.3d at 306-08 (surveying cases); see also, e.g., *Black v. United States*, 62 F.3d 1115, 1117-20 (8th Cir. 1995); *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544, 548 (2d Cir. 1991).

Kasza is not to the contrary. While this Court in *Kasza* affirmed the dismissal of the case because its very subject matter was a state secret (133 F.3d at 1170), it did not suggest, much less hold, that dismissal would be inappropriate at the outset for other reasons. To the contrary, the Court recognized that judgment for the Government is also warranted where “the privilege deprives the *defendant* of information that would otherwise give the defendant a valid defense to the claim.” *Id.* at 1066. As explained above, and in the Government’s motion to dismiss or, in

the alternative, for summary judgment, that rationale alone compels dismissal here because state secrets would prevent litigation of plaintiffs' standing and the merits.

Plaintiffs assert that a different situation might be presented "if in the future the Government invokes the state secrets privilege with respect to specific evidence." Br. 58. But the Government has already asserted the privilege with respect to the categories of evidence that plaintiffs would need to prove (and AT&T would need to refute) standing and the merits. Delaying dismissal would serve only to jeopardize national security through further proceedings in a case that could not proceed to judgment—a pointless and dangerous endeavor that the state secrets privilege is designed to prevent.

2. Regarding the minimum Article III requirement of standing, plaintiffs do not appear to dispute that their standing to challenge alleged past interceptions depends on whether, at a minimum, they can establish that "at least one" of each plaintiffs' communications was intercepted. See Br. 71-72, 76-77. To prove standing, plaintiffs would therefore have to show that (1) the alleged "dragnet" program exists, (2) AT&T participated in the program, and (3) plaintiffs' communications were in fact intercepted. Plaintiffs have not made, and cannot make, that showing.

Plaintiffs instead assert that they need only *allege* such interceptions, and that their central allegation of a content "dragnet" does so. See Br. 70-80. But allegations are insufficient by themselves to withstand dismissal when invocation of the state

secrets privilege demonstrates that the allegations cannot be litigated—for purposes of establishing standing or testing the merits—without jeopardizing state secrets. As the D.C. Circuit has explained, allegations that a plaintiff’s communications have been intercepted could constitute an injury in fact if proven, but the “sufficiency of *those allegations* must * * * be reevaluated” once the Government’s assertion of the state secrets privilege prevents presentation of evidence needed to substantiate them. See *Halkin v. Helms*, 690 F.2d 977, 999 (D.C. Cir. 1982) (“*Halkin II*”) (emphasis added).

Moreover, even under plaintiffs’ reading of the record, their evidence suggests at most that “all or substantially all” WorldNet internet traffic from a relevant area was diverted. Br. 76-77. No evidence exists that any of the four plaintiffs’ own communications were, in fact, intercepted. Plaintiffs argue that, to establish injury in fact, they need only prove a “likelihood that their *past* communications were intercepted” (Br. 77-78 & n.15). That is incorrect. Plaintiffs point to cases, outside the surveillance context, challenging the legality of past actions where litigants based their standing on the likelihood that those past acts would cause them future injury. Here, however, the alleged past acts of interception whose legality plaintiffs wish to challenge *are* the very injury upon which plaintiffs must base their standing. That injury either did or did not occur, and, as courts have recognized in similar challenges to alleged surveillance, it is plaintiffs’ burden to prove that it did. See, e.g., *Halkin II*, 690 F.2d at 991, 999. Because the state secrets privilege prevents litigation over what

communications, if any, were intercepted, plaintiffs' challenge to alleged past surveillance must be dismissed for lack of standing.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 19]

Plaintiffs likewise cannot establish standing for prospective relief regarding the *future* interception of communications. Case precedent requires plaintiffs challenging a surveillance program to establish that they have already been subject to surveillance, and no reason exists to dispense with that settled requirement. In any event, plaintiffs cannot establish that they face a realistic future threat from ongoing surveillance without court approval, because any electronic surveillance previously conducted as part of the TSP is now being conducted subject to the FISA Court’s approval. See Gov. Br. 9-10, 43-44 n.3. Plaintiffs instead argue that they have standing for injunctive relief from future *untargeted* “dragnet” surveillance, because the Government has “never suggested that it has secured or ever sought [court] authorization for the dragnet surveillance at issue in this case.” Br. 70. But plaintiffs cannot prove any such likelihood without recourse to state secrets concerning the existence and scope (including targeting) of the alleged “dragnet.”

3. On the merits, plaintiffs argue that all they “have to prove is the unrevealing and well-known fact that AT&T intercepted or disclosed their communications and records—and did so without following statutory procedures.” Br. 52. To prevail on their claims, plaintiffs would need to prove more than that. See Gov. Br. 37-46. In any event, litigation concerning AT&T’s alleged interceptions or disclosures would require the Government to reveal state secrets to prove its denial of the alleged “dragnet,” including any AT&T involvement.

Indeed, as plaintiffs elsewhere acknowledge (Br. 61), the central question of whether a secret relationship exists between AT&T and the Government is essential to plaintiffs' ability to prove their claims and AT&T's ability to establish defenses. See Gov. Br. 44-46. But as stressed by General Alexander and Director Negroponete, the Government's state secrets assertion squarely encompasses the question of "NSA's purported involvement with AT&T"; "[t]he United States can neither confirm nor deny allegations concerning intelligence * * * relationships"; and any such confirmation or denial "could reasonably be expected to cause exceptionally grave damage to the national security." ER 57-59; see ER 63-64. Thus, the question of the existence and extent of any relationship between AT&T and the Government regarding the alleged activities falls within the heartland of the state secrets privilege.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 21]

III. CONGRESS HAS NOT ABROGATED THE STATE SECRETS PRIVILEGE.

Finally, plaintiffs revive a novel and far-reaching argument that the district court did not accept: that Congress abrogated the state secrets privilege under FISA. Br. 27-36, 48-49; ER 329. That argument is contradicted by the text and legislative history of FISA, as well as settled rules of statutory construction.

A. For several reasons, Congress could not abrogate the state secrets privilege without (at a minimum) clearly stating its intent to do so. First, the privilege has “a firm foundation in the Constitution, in addition to its basis in the common law of evidence.” *El-Masri*, 479 F.3d at 303-04. The privilege stems from the Article II power over military and foreign affairs, where the “Executive’s constitutional authority is at its broadest.” See *ibid.* (citing *United States v. Nixon*, 418 U.S. 683, 710 (1974)); see also Gov. Br. 15. Plaintiffs disregard the privilege’s constitutional foundation, and make no attempt to grapple with the serious constitutional questions that would arise if Section 1806(f) of FISA were read to abrogate the privilege, and thereby impair the President’s ability to protect vital military and intelligence secrets from public disclosure. The constitutional avoidance doctrine counsels that Section 1806(f) be construed to avoid such difficulties “unless such construction is plainly contrary to the intent of Congress.” See *Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988). The “clear

statement doctrine” similarly requires that statutes not be read to interfere with the President’s powers unless Congress has made clear an intent to confront the ensuing constitutional questions. See *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C. Cir. 1991).

Second, in addition to its constitutional foundation, the state secrets privilege is deeply rooted at common law. *Kasza*, 133 F.3d at 1167. ““The common law * * * ought not to be deemed repealed, unless the language of a statute be clear and explicit for this purpose.”” *Norfolk Redevelopment & Housing Auth. v. Chesapeake & Potomac Tel. Co.*, 464 U.S. 30, 35 (1983); see *Kasza*, 133 F.3d at 1167. Therefore, there would be no basis to conclude that Congress abrogated the state secrets privilege unless it did so in “clear and explicit” terms.

Third, Section 6 of the National Security Agency Act of 1959 mandates that “nothing in this Act or *any other law* * * * *shall be construed* to require the disclosure * * * of any information with respect to the activities” of the NSA. See 50 U.S.C. 402 note (emphasis added). This anti-disclosure provision is “absolute” (*Linder v. National Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996)), and its “plain text unequivocally demonstrates that Congress intended to prevent” the radical interpretation of FISA that plaintiffs advance with respect to alleged surveillance activities undertaken by the NSA. See *California v. United States*, 215 F.3d 1005, 1009 n.3, 1011 & n.4 (9th Cir. 2000) (construing similar text).

B. Nothing in FISA explicitly abrogates the state secrets privilege. Indeed, far from providing the requisite clear intent to displace the privilege, FISA limits the circumstances in which surveillance may be publicly disclosed. Section 1806(f) provides aggrieved persons with a shield against the Government’s affirmative use of information obtained from disclosed, unlawful electronic surveillance. Located within FISA’s provision governing the “[u]se of information” obtained from surveillance (50 U.S.C. 1806), subsection (f) limits itself to three situations in which the potential use of surveillance-based information in proceedings against an aggrieved person requires a judicial determination of whether the underlying surveillance was lawful:

(1) the Government provides notice that it “intends to enter into evidence or otherwise use or disclose” surveillance-based information in judicial or administrative proceedings against an aggrieved person (see 50 U.S.C. 1806(c), (d));

(2) the “aggrieved person” moves in such proceedings to suppress “evidence [or information] obtained or derived from an electronic surveillance” (see § 1806(e), (f)); or

(3) the “aggrieved person” moves to “discover or obtain” “applications, orders, or other materials relating to electronic surveillance” or “evidence or information obtained or derived from electronic surveillance.”

See 50 U.S.C. 1806(f); see also *ACLU Found. v. Barr*, 952 F.2d 457, 462 (D.C. Cir. 1991).

Each of subsection (f)’s limitations is premised on the fact that electronic surveillance has already been disclosed. Notice of the intended use of surveillance-

based evidence necessarily discloses the fact of surveillance. Similarly, a motion to suppress such evidence occurs only after the fact of surveillance is established. Congress recognized that suppression motions “most common[ly]” would arise after a litigant “discovers that he has been intercepted by electronic surveillance” from a Governmental admission, but could also arise after a court orders surveillance-related materials disclosed to the litigant in order to determine whether the surveillance was lawful, or a litigant obtains new evidence after an initial determination of lawfulness. See S. Rep. No. 95-701, at 62-63 (1978).

Likewise, requests to “discover or obtain” evidence or information relating to or derived from surveillance are predicated on disclosed surveillance. Congress specified that such requests must be “made by an aggrieved person,” which requires the movant to have established that he was a “*target of an electronic surveillance*” or a “person whose communications or activities were *subject to electronic surveillance.*” See 50 U.S.C. 1801(k), 1806(f) (emphasis added). Congress contemplated that, if a district court found the underlying surveillance unlawful under Section 1806(f), it would grant such motions “in accordance with the requirements of law” (Section 1806(g)), and, in certain proceedings, require the Government “to surrender to the defendant all the records of the surveillance in its possession” to “assist him in establishing the existence of ‘taint.’” See S. Rep. No. 95-701, at 65; see also S. Rep. No. 95-604, at 59 n.61 (1977).

Under FISA’s framework, an individual is entitled to relief only if he is defending Government-initiated proceedings where it is established that he is an “aggrieved person” and that the surveillance was unlawful. Under plaintiffs’ view, however, a plaintiff could obtain the relief requested—discovery of surveillance—in order to prove that he was an aggrieved person and was therefore entitled to discovery of the surveillance. This argument turns FISA’s “aggrieved person” requirement on its head, and threatens grave harm to national security because any potential target of FISA-authorized or other surveillance could force disclosure of sensitive intelligence-gathering by simply alleging, on information and belief, to be aggrieved (much as plaintiffs have done here). FISA, however, requires the Government to provide notice only when it intends to use the fruits of the surveillance against a person. 50 U.S.C. 1806(c). Otherwise, FISA is structured to *preserve* the confidentiality, and thus effectiveness, of intelligence-gathering. See, e.g., 50 U.S.C. 1805(a) (*ex parte* orders), 1806(j).

That Section 1806(f) applies only when surveillance has been disclosed is further reflected by the determination that a district court must make under Section 1806(f), *i.e.*, “whether *the surveillance* of the aggrieved person was lawfully authorized and conducted” based on the court’s review of “materials relating to *the surveillance.*” The use of the direct article “the,” like the use of “aggrieved person,” illustrates that Congress treated the existence of disclosed surveillance (and, thus, an

“aggrieved person”) as a predicate for Section 1806(f), and did not intend Section 1806(f) to be used as a free-standing vehicle to allow litigants to test mere allegations of surveillance.

This statutory emphasis on “the surveillance” in FISA contrasts significantly with other statutory provisions governing “*alleged*” surveillance. For instance, 18 U.S.C. 3504 specifies that the Government “shall affirm or deny the occurrence of the *alleged* unlawful [surveillance]” when a litigant in judicial or administrative proceedings properly supports a claim that the Government’s evidence in such proceedings is inadmissible as the product of unlawful surveillance. 18 U.S.C. 3504(a)(1), (b) (emphasis added); see *In re Grand Jury Investigation*, 437 F.3d 855, 856 (9th Cir. 2006); *United States v. Tobias*, 836 F.2d 449, 452-53 (9th Cir. 1988). Congress thus specifically designed Section 1806(f) to be used *after* a defendant “discovers that he has been intercepted by electronic surveillance” under Section 3504. S. Rep. No. 95-701, at 63.

ACLU Foundation underscores this point. There, the Government disclosed the occurrence of specific surveillance activity in response to a Section 3504 motion filed by aliens in deportation proceedings, and thereafter utilized Section 1806(f) to establish the legality of the surveillance (and eliminate any claim of access to its fruits). See 952 F.2d at 460, 462-63; cf. *id.* at 469. Because two other plaintiffs did not benefit from this Section 3504 admission, the D.C. Circuit concluded that they

would have to “prov[e] ongoing surveillance” and the other facts necessary for their case without discovery from the Government, which, the Court ruled, “has no duty to reveal ongoing foreign intelligence surveillance.” See *id.* at 466 n.10, 468-69 & n.13.

C. FISA’s legislative history confirms that Section 1806(f) does not abrogate the state secrets privilege. Congress crafted Section 1806(f) to strike a “balance” between the aggrieved person’s “ability to defend himself” against the Government’s use of the legal process, and the need to protect “sensitive foreign intelligence information” from disclosure. See S. Rep. No. 95-701, at 64; cf. H.R. Conf. Rep. No. 95-1720, at 31-32 (1978) (adopting Senate’s framework for Section 1806(f)). Congress thus recognized that the “need to preserve secrecy for sensitive counterintelligence sources and methods” would make “notice [of surveillance] to the surveillance target” inappropriate “*unless the fruits are to be used against him in legal proceedings.*” S. Rep. No. 95-701, at 11-12 (emphasis added). And, even where a court orders information disclosed to the aggrieved person, Congress gave the Government a choice: “either disclose the material or forgo the use of the surveillance-based evidence.” S. Rep. No. 95-701, at 65.

Instead of abrogating the state secrets privilege, Section 1806(f) addresses issues different from than those implicated by the state secrets privilege. That privilege provides the Government with a shield where disclosure of information could reveal state secrets. It applies only when “the political head of the department”

controlling the information (here, the Director of National Intelligence) asserts the privilege based on his “personal consideration” and his determination that ““on grounds of public interest [it] ought not be produced.”” See *United States v. Reynolds*, 345 U.S. 1, 7-8 & n.20 (1953). Section 1806(f)’s *in camera* procedure, in contrast, applies when the Government seeks to use or otherwise discloses the fruits of surveillance, and it is invoked not by the “head” of the department with control over the relevant surveillance information, but by the Attorney General or subordinate officials (50 U.S.C. 1801(g), 1806(f)), because the Department of Justice is ultimately responsible for litigation where the Government may utilize surveillance-based information as a sword. Cf. 28 U.S.C. 514, 516, 519.

* * * * *

Plaintiffs are relegated to suggesting that the state secrets privilege cannot apply to broad (even if unsubstantiated) allegations of constitutional violations. See Br. 55-57. The breadth of the allegations here only underscores the magnitude of the harm that could result from disclosure. And where the elements of the privilege are met, “the state secrets doctrine finds the greater public good—ultimately the less harsh remedy—to be dismissal.” *Kasza*, 133 F.3d at 1167. Indeed, that is the “result required” even where allegations of unlawful or unconstitutional actions are at issue. *Halkin II*, 690 F.2d at 1001. Plaintiffs’ alleged interests are not the only ones at stake; the constitutional interests are not one-sided (see U.S. Const. pmb., art. II, § 2); and

litigating a case such as this, whose very subject matter is a state secret, would lead to a harsh result of another kind—one that could potentially harm the security of all Americans. See, e.g., *El-Masri*, 479 F.3d at 313.

CONCLUSION

For the foregoing reasons, and those in our opening brief, the district court's decision should be reversed and this case dismissed.

Respectfully submitted,

PAUL D. CLEMENT
Solicitor General

GREGORY G. GARRE
Deputy Solicitor General

DARYL JOSEFFER
Assistant to the Solicitor
General

PETER D. KEISLER
Assistant Attorney General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

Douglas N. Letter
Thomas M. Bondy
Anthony A. Yang

MAY 2007

ADDENDUM

ADDENDUM TABLE OF CONTENTS

Page

Foreign Intelligence Surveillance Act of 1978, as amended,
50 U.S.C. 1801-1871

50 U.S.C. 1801	1a
50 U.S.C. 1806	2a

National Security Agency Act of 1959,
Pub. L. No. 86-36, 73 Stat. 63 (1959)

Section 6 (50 U.S.C. § 402 note)	4a
--	----

18 U.S.C. 3504	5a
----------------------	----

Foreign Intelligence Surveillance Act of 1978, as amended
50 U.S.C. 1801-1871

50 U.S.C. 1801

§ 1801. Definitions

As used in this subchapter:

* * * *

(g) “Attorney General” means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

* * * *

(k) “Aggrieved person” means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

* * * *

50 U.S.C. 1806**§ 1806. Use of information**

* * * *

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

- (1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

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

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

* * * *

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of—

- (1) the fact of the application;
- (2) the period of the surveillance; and
- (3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

* * * *

National Security Agency Act of 1959
Pub. L. No. 86-36, 73 Stat. 63

* * * *

Sec. 6. (a) Except as provided in subsection (b) of this section, nothing in this Act or any other law (including, but not limited to, the first section and section 2 of the Act of August 28, 1935 (5 U.S.C. 654)) shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

(b) The reporting requirements of section 1582 of title 10, United States Code, shall apply to positions established in the National Security Agency in the manner provided by section 4 of this Act.

* * * *

18 U.S.C. 3504

§ 3504. Litigation concerning sources of evidence

(a) In any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority of the United States—

(1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act;

(2) * * * ; and

(3) * * * .

(b) As used in this section “unlawful act” means any act the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto.

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief is in compliance with Rule 32(a)(7) of the Federal Rules of Appellate Procedure. The public and classified versions of this brief contain no more than 7,000 words, and were prepared in 14-point Times New Roman font using Corel WordPerfect 12.0.

CERTIFICATE OF SERVICE

I further certify that on this 24th day of May, 2007, I caused to be served via Federal Express two true and correct copies of the foregoing reply brief properly addressed to the following:

Robert D. Fram, Esq.
Michael M. Markman, Esq.
Heller Ehrman, LLP
333 Bush Street
San Francisco, CA 94104-2878
415-772-6000
Counsel for Plaintiffs-Appellees

Bradford A. Berenson, Esq.
David Lawson, Esq.
Edward R. McNicholas, Esq.
Sidley Austin, LLP
1501 K Street, NW
Washington, DC 20005
202-736-8010
Counsel for Defendants


Anthony A. Yang