



- 1 (2) Section 109 of Title I of the Foreign Intelligence  
2 Surveillance Act of 1978 (FISA), 50 USC § 1809, by  
3 engaging in illegal electronic surveillance of  
4 plaintiffs' communications under color of law;
- 5 (3) Section 802 of Title III of the Omnibus Crime Control and  
6 Safe Streets Act of 1968, as amended by section 101 of  
7 Title I of the Electronic Communications Privacy Act of  
8 1986 (ECPA), 18 USC §§ 2511(1)(a), (1)(c), (1)(d) and  
9 (3)(a), by illegally intercepting, disclosing, using  
10 and/or divulging plaintiffs' communications;
- 11 (4) Section 705 of Title VII of the Communications Act of  
12 1934, as amended, 47 USC § 605, by unauthorized  
13 divulgence and/or publication of plaintiffs'  
14 communications;
- 15 (5) Section 201 of Title II of the ECPA ("Stored  
16 Communications Act"), as amended, 18 USC §§ 2702(a)(1)  
17 and (a)(2), by illegally divulging the contents of  
18 plaintiffs' communications;
- 19 (6) Section 201 of the Stored Communications Act, as amended  
20 by section 212 of Title II of the USA PATRIOT Act, 18 USC  
21 § 2702(a)(3), by illegally divulging records concerning  
22 plaintiffs' communications to a governmental entity and
- 23 (7) California's Unfair Competition Law, Cal Bus & Prof Code  
24 §§ 17200 et seq, by engaging in unfair, unlawful and  
25 deceptive business practices.

26 The complaint seeks certification of a class action and redress  
27 through statutory damages, punitive damages, restitution,  
28 disgorgement and injunctive and declaratory relief.

1           On April 5, 2006, plaintiffs moved for a preliminary  
2 injunction seeking to enjoin defendants' allegedly illegal  
3 activity. Doc #30 (MPI). Plaintiffs supported their motion by  
4 filing under seal three documents, obtained by former AT&T  
5 technician Mark Klein, which allegedly demonstrate how AT&T has  
6 implemented a warrantless surveillance system on behalf of the NSA  
7 at a San Francisco AT&T facility. Doc #31, Exs A-C (the "AT&T  
8 documents"). Plaintiffs also filed under seal supporting  
9 declarations from Klein (Doc #31) and J Scott Marcus (Doc #32), a  
10 putative expert who reviewed the AT&T documents and the Klein  
11 declaration.

12           On April 28, 2006, AT&T moved to dismiss this case. Doc  
13 #86 (AT&T MTD). AT&T contends that plaintiffs lack standing and  
14 were required but failed to plead affirmatively that AT&T did not  
15 receive a government certification pursuant to 18 USC §  
16 2511(2)(a)(ii)(B). AT&T also contends it is entitled to statutory,  
17 common law and qualified immunity.

18           On May 13, 2006, the United States moved to intervene as  
19 a defendant and moved for dismissal or, alternatively, for summary  
20 judgment based on the state secrets privilege. Doc #124-1 (Gov  
21 MTD). The government supported its assertion of the state secrets  
22 privilege with public declarations from the Director of National  
23 Intelligence, John D Negroponte (Doc #124-2 (Negroponte Decl)), and  
24 the Director of the NSA, Keith B Alexander (Doc #124-3 (Alexander  
25 Decl), and encouraged the court to review additional classified  
26 submissions *in camera* and *ex parte*. The government also asserted  
27 two statutory privileges under 50 USC § 402 *note* and 50 USC § 403-  
28 1(i)(1).



1 surveillance activities. Finally, the court addresses the  
2 statutory privileges raised by the government.

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

A

"The state secrets privilege is a common law evidentiary rule that protects information from discovery when disclosure would be inimical to the national security. Although the exact origins of the privilege are not certain, the privilege in this country has its initial roots in Aaron Burr's trial for treason, and has its modern roots in United States v Reynolds, 345 US 1 (1953)." In re United States, 872 F2d 472, 474-75 (DC Cir 1989) (citations omitted and altered). In his trial for treason, Burr moved for a *subpoena duces tecum* ordering President Jefferson to produce a letter by General James Wilkinson. United States v Burr, 25 F Cas 30, 32 (CCD Va 1807). Responding to the government's argument "that the letter contains material which ought not to be disclosed," Chief Justice Marshall riding circuit noted, "What ought to be done under such circumstances presents a delicate question, the discussion of which, it is hoped, will never be rendered necessary in this country." *Id* at 37. Although the court issued the subpoena, *id* at 37-38, it noted that if the letter "contain[s] any matter which it would be imprudent to disclose, which it is not the wish of the executive to disclose, such matter, if it be not immediately and essentially applicable to the point, will, of course, be suppressed." *Id* at 37.

//  
//  
//

1           The actions of another president were at issue in Totten  
2 v United States, 92 US 105 (1876), in which the Supreme Court  
3 established an important precursor to the modern-day state secrets  
4 privilege. In that case, the administrator of a former spy's  
5 estate sued the government based on a contract the spy allegedly  
6 made with President Lincoln to recover compensation for espionage  
7 services rendered during the Civil War. Id at 105-06. The Totten  
8 Court found the action to be barred:

9           The service stipulated by the contract was a secret  
10 service; the information sought was to be obtained  
11 clandestinely, and was to be communicated  
12 privately; the employment and the service were to  
13 be equally concealed. Both employer and agent must  
14 have understood that the lips of the other were to  
15 be for ever sealed respecting the relation of  
16 either to the matter. This condition of the  
17 engagement was implied from the nature of the  
18 employment, and is implied in all secret  
19 employments of the government in time of war, or  
20 upon matters affecting our foreign relations, where  
21 a disclosure of the service might compromise or  
22 embarrass our government in its public duties, or  
23 endanger the person or injure the character of the  
24 agent.

25 Id at 106, quoted in Tenet v Doe, 544 US 1, 7-8 (2005). Hence,  
26 given the secrecy implied in such a contract, the Totten Court  
27 "thought it entirely incompatible with the nature of such a  
28 contract that a former spy could bring suit to enforce it." Tenet,  
544 US at 8. Additionally, the Totten Court observed:

It may be stated as a 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, and  
respecting which it will not allow the confidence  
to be violated. \* \* \* Much greater reason exists  
for the application of the principle to cases of  
contract for secret services with the government,  
as the existence of a contract of that kind is  
itself a fact not to be disclosed.

1 Totten, 92 US at 107. Characterizing this aspect of Totten, the  
2 Supreme Court has noted, "No matter the clothing in which alleged  
3 spies dress their claims, Totten precludes judicial review in cases  
4 such as [plaintiffs'] where success depends upon the existence of  
5 their secret espionage relationship with the Government." Tenet,  
6 544 US at 8. "Totten's core concern" is "preventing the existence  
7 of the [alleged spy's] relationship with the Government from being  
8 revealed." *Id* at 10.

9 In the Cold War era case of Reynolds v United States, 345  
10 US 1 (1953), the Supreme Court first articulated the state secrets  
11 privilege in its modern form. After a B-29 military aircraft  
12 crashed and killed three civilian observers, their widows sued the  
13 government under the Federal Tort Claims Act and sought discovery  
14 of the Air Force's official accident investigation. *Id* at 2-3.  
15 The Secretary of the Air Force filed a formal "Claim of Privilege"  
16 and the government refused to produce the relevant documents to the  
17 court for *in camera* review. *Id* at 4-5. The district court deemed  
18 as established facts regarding negligence and entered judgment for  
19 plaintiffs. *Id* at 5. The Third Circuit affirmed and the Supreme  
20 Court granted certiorari to determine "whether there was a valid  
21 claim of privilege under [FRCP 34]." *Id* at 6. Noting this  
22 country's theretofore limited judicial experience with "the  
23 privilege which protects military and state secrets," the court  
24 stated:

25 //  
26 //  
27 //  
28 //

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

The privilege belongs to the Government and must be asserted by it \* \* \*. It is not to be lightly invoked. There must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer. The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect.

Id at 7-8 (footnotes omitted). The latter determination requires a "formula of compromise," as "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers," yet a court may not "automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case." Id at 9-10. Striking this balance, the Supreme Court held that the "occasion for the privilege is appropriate" when a court is satisfied "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." Id at 10.

The degree to which the court may "probe in satisfying itself that the occasion for invoking the privilege is appropriate" turns on "the showing of necessity which is made" by plaintiffs. Id at 11. "Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake." Id. Finding both a "reasonable danger that the accident investigation report would contain" state secrets and a "dubious showing of necessity," the court reversed the Third Circuit's decision and sustained the claim of privilege. Id at 10-12.



1 In Halkin v Helms, 598 F2d 1 (DC Cir 1978) (Halkin I),  
2 the District of Columbia Circuit applied the principles enunciated  
3 in Reynolds in an action alleging illegal NSA wiretapping. Former  
4 Vietnam War protestors contended that "the NSA conducted  
5 warrantless interceptions of their international wire, cable and  
6 telephone communications" at the request of various federal  
7 defendants and with the cooperation of telecommunications  
8 providers. *Id* at 3. Plaintiffs challenged two separate NSA  
9 operations: operation MINARET, which was "part of [NSA's] regular  
10 signals intelligence activity in which foreign electronic signals  
11 were monitored," and operation SHAMROCK, which involved "processing  
12 of all telegraphic traffic leaving or entering the United States."  
13 *Id* at 4.

14 The government moved to dismiss on state secrets grounds,  
15 arguing that civil discovery would impermissibly "(1) confirm the  
16 identity of individuals or organizations whose foreign  
17 communications were acquired by NSA, (2) disclose the dates and  
18 contents of such communications, or (3) divulge the methods and  
19 techniques by which the communications were acquired by NSA." *Id*  
20 at 4-5. After plaintiffs "succeeded in obtaining a limited amount  
21 of discovery," the district court concluded that plaintiffs' claims  
22 challenging operation MINARET could not proceed because "the  
23 ultimate issue, the fact of acquisition, could neither be admitted  
24 nor denied." *Id* at 5. The court denied the government's motion to  
25 dismiss on claims challenging operation SHAMROCK because the court  
26 "thought congressional committees investigating intelligence  
27 matters had revealed so much information about SHAMROCK that such a  
28 disclosure would pose no threat to the NSA mission." *Id* at 10.

1 On certified appeal, the District of Columbia Circuit  
2 noted that even "seemingly innocuous" information is privileged if  
3 that information is part of a classified "mosaic" that "can be  
4 analyzed and fitted into place to reveal with startling clarity how  
5 the unseen whole must operate." Id at 8. The court affirmed  
6 dismissal of the claims related to operation MINARET but reversed  
7 the district court's rejection of the privilege as to operation  
8 SHAMROCK, reasoning that "confirmation or denial that a particular  
9 plaintiff's communications have been acquired would disclose NSA  
10 capabilities and other valuable intelligence information to a  
11 sophisticated intelligence analyst." Id at 10. On remand, the  
12 district court dismissed plaintiffs' claims against the NSA and  
13 individuals connected with the NSA's alleged monitoring.  
14 Plaintiffs were left with claims against the Central Intelligence  
15 Agency (CIA) and individuals who had allegedly submitted watchlists  
16 to the NSA on the presumption that the submission resulted in  
17 interception of plaintiffs' communications. The district court  
18 eventually dismissed the CIA-related claims as well on state  
19 secrets grounds and the case went up again to the court of appeals.

20 The District of Columbia Circuit stated that the state  
21 secrets inquiry "is not a balancing of ultimate interests at stake  
22 in the litigation," but rather "whether the showing of the harm  
23 that might reasonably be seen to flow from disclosure is adequate  
24 in a given case to trigger the absolute right to withhold the  
25 information sought in that case." Halkin v Helms, 690 F2d 977, 990  
26 (DC Cir 1982) (Halkin II). The court then affirmed dismissal of  
27 "the claims for injunctive and declaratory relief against the CIA  
28 defendants based upon their submission of plaintiffs' names on

1 'watchlists' to NSA." Id at 997 (emphasis omitted). The court  
2 found that plaintiffs lacked standing given the court's "ruling in  
3 Halkin I that evidence of the fact of acquisition of plaintiffs'  
4 communications by NSA cannot be obtained from the government, nor  
5 can such fact be presumed from the submission of watchlists to that  
6 Agency." Id at 999 (emphasis omitted).

7 In Ellsberg v Mitchell, 709 F2d 51 (DC Cir 1983), the  
8 District of Columbia Circuit addressed the state secrets privilege  
9 in another wiretapping case. Former defendants and attorneys in  
10 the "Pentagon Papers" criminal prosecution sued individuals who  
11 allegedly were responsible for conducting warrantless electronic  
12 surveillance. Id at 52-53. In response to plaintiffs'  
13 interrogatories, defendants admitted to two wiretaps but refused to  
14 answer other questions on the ground that the requested information  
15 was privileged. Id at 53. The district court sustained the  
16 government's formal assertion of the state secrets privilege and  
17 dismissed plaintiffs' claims pertaining to foreign communications  
18 surveillance. Id at 56.

19 On appeal, the District of Columbia Circuit noted that  
20 "whenever possible, sensitive information must be disentangled from  
21 nonsensitive information to allow for the release of the latter."  
22 Id at 57. The court generally affirmed the district court's  
23 decisions regarding the privilege, finding "a 'reasonable danger'  
24 that revelation of the information in question would either enable  
25 a sophisticated analyst to gain insights into the nation's  
26 intelligence-gathering methods and capabilities or would disrupt  
27 diplomatic relations with foreign governments." Id at 59. The  
28 court disagreed with the district court's decision that the

1 privilege precluded discovery of the names of the attorneys general  
2 that authorized the surveillance. Id at 60.

3           Additionally, responding to plaintiffs' argument that the  
4 district court should have required the government to disclose more  
5 fully its basis for asserting the privilege, the court recognized  
6 that "procedural innovation" was within the district court's  
7 discretion and noted that "[t]he government's public statement need  
8 be no more (and no less) specific than is practicable under the  
9 circumstances." Id at 64.

10           In considering the effect of the privilege, the court  
11 affirmed dismissal "with regard to those [individuals] whom the  
12 government ha[d] not admitted overhearing." Id at 65. But the  
13 court did not dismiss the claims relating to the wiretaps that the  
14 government had conceded, noting that there was no reason to  
15 "suspend the general rule that the burden is on those seeking an  
16 exemption from the Fourth Amendment warrant requirement to show the  
17 need for it." Id at 68.

18           In Kasza v Browner, 133 F3d 1159 (9th Cir 1998), the  
19 Ninth Circuit issued its definitive opinion on the state secrets  
20 privilege. Former employees at a classified United States Air  
21 Force facility brought a citizen suit under the Resource  
22 Conservation and Recovery Act (RCRA), 42 USC § 6972, alleging the  
23 Air Force violated that act. Id at 1162. The district court  
24 granted summary judgment against plaintiffs, finding discovery of  
25 information related to chemical inventories impossible due to the  
26 state secrets privilege. Id. On appeal, plaintiffs argued that an  
27 exemption in the RCRA preempted the state secrets privilege and  
28 even if not preempted, the privilege was improperly asserted and

1 too broadly applied. Id at 1167-69. After characterizing the  
2 state secrets privilege as a matter of federal common law, the  
3 Ninth Circuit recognized that "statutes which invade the common law  
4 \* \* \* are to be read with a presumption favoring the retention of  
5 long-established and familiar principles, except when a statutory  
6 purpose to the contrary is evident." Id at 1167 (omissions in  
7 original) (citations omitted). Finding no such purpose, the court  
8 held that the statutory exemption did not preempt the state secrets  
9 privilege. Id at 1168.

10 Kasza also explained that the state secrets privilege can  
11 require dismissal of a case in three distinct ways. "First, by  
12 invoking the privilege over particular evidence, the evidence is  
13 completely removed from the case. The plaintiff's case then goes  
14 forward based on evidence not covered by the privilege. \* \* \* If,  
15 after further proceedings, the plaintiff cannot prove the *prima*  
16 *facie* elements of her claim with nonprivileged evidence, then the  
17 court may dismiss her claim as it would with any plaintiff who  
18 cannot prove her case." Id at 1166. Second, "if the privilege  
19 deprives the defendant of information that would otherwise give the  
20 defendant a valid defense to the claim, then the court may grant  
21 summary judgment to the defendant." Id (internal quotation  
22 omitted) (emphasis in original). Finally, and most relevant here,  
23 "notwithstanding the plaintiff's ability to produce nonprivileged  
24 evidence, if the 'very subject matter of the action' is a state  
25 secret, then the court should dismiss the plaintiff's action based  
26 solely on the invocation of the state secrets privilege." Id  
27 (quoting Reynolds, 345 US at 11 n26). See also Reynolds, 345 US at  
28 11 n26 (characterizing Totten as a case "where the very subject

1 matter of the action, a contract to perform espionage, was a matter  
2 of state secret. The action was dismissed on the pleadings without  
3 ever reaching the question of evidence, since it was so obvious  
4 that the action should never prevail over the privilege.”).

5 According the “utmost deference” to the government’s  
6 claim of privilege and noting that even “seemingly innocuous  
7 information” could be “part of a classified mosaic,” *id* at 1166,  
8 Kasza concluded after *in camera* review of classified declarations  
9 “that release of such information would reasonably endanger  
10 national security interests.” *Id* at 1170. Because “no protective  
11 procedure” could salvage plaintiffs’ case, and “the very subject  
12 matter of [her] action [was] a state secret,” the court affirmed  
13 dismissal. *Id*.

14 More recently, in Tenet v Doe, 544 US 1 (2005), the  
15 Supreme Court reaffirmed Totten, holding that an alleged former  
16 Cold War spy could not sue the government to enforce its  
17 obligations under a covert espionage agreement. *Id* at 3.  
18 Importantly, the Court held that Reynolds did not “replac[e] the  
19 categorical Totten bar with the balancing of the state secrets  
20 evidentiary privilege in the distinct class of cases that depend  
21 upon clandestine spy relationships.” *Id* at 9-10.

22 Even more recently, in El-Masri v Tenet, 2006 WL 1391390,  
23 05-cv-01417 (ED Va May 12, 2006), plaintiff sued the former  
24 director of the CIA and private corporations involved in a program  
25 of “extraordinary rendition,” pursuant to which plaintiff was  
26 allegedly beaten, tortured and imprisoned because the government  
27 mistakenly believed he was affiliated with the al Qaeda terrorist  
28 organization. *Id* at \*1-2. The government intervened “to protect

1 its interests in preserving state secrets." Id at \*3. The court  
2 sustained the government's assertion of the privilege:

3 [T]he substance of El-Masri's publicly available  
4 complaint alleges a clandestine intelligence  
5 program, and the means and methods the foreign  
6 intelligence services of this and other countries  
7 used to carry out the program. And, as the public  
8 declaration makes pellucidly clear, any admission  
9 or denial of these allegations by defendants \* \* \*  
10 would present a grave risk of injury to national  
11 security.

12 Id at \*5. The court also rejected plaintiff's argument "that  
13 government officials' public affirmation of the existence" of the  
14 rendition program somehow undercut the claim of privilege because  
15 the government's general admission provided "no details as to the  
16 [program's] means and methods," which were "validly claimed as  
17 state secrets." Id. Having validated the exercise of privilege,  
18 the court reasoned that dismissal was required because "any answer  
19 to the complaint by the defendants risk[ed] the disclosure of  
20 specific details [of the program]" and special discovery procedures  
21 would have been "plainly ineffective where, as here, the entire aim  
22 of the suit [was] to prove the existence of state secrets." Id at  
23 \*6.

24 B

25 Relying on Kasza, the government advances three reasons  
26 why the state secrets privilege requires dismissing this action or  
27 granting summary judgment for AT&T: (1) the very subject matter of  
28 this case is a state secret; (2) plaintiffs cannot make a *prima*  
*facie* case for their claims without classified evidence and (3) the  
privilege effectively deprives AT&T of information necessary to  
raise valid defenses. Doc #245-1 (Gov Reply) at 3-5.

1 In support of its contention that the very subject matter  
2 of this action is a state secret, the government argues: "AT&T  
3 cannot even confirm or deny the key factual premise underlying  
4 [p]laintiffs' entire case -- that AT&T has provided any assistance  
5 whatsoever to NSA regarding foreign-intelligence surveillance.  
6 Indeed, in the formulation of Reynolds and Kasza, that allegation  
7 is 'the very subject of the action.'" Id at 4-5.

8 Additionally, the government claims that dismissal is  
9 appropriate because plaintiffs cannot establish a *prima facie* case  
10 for their claims. Contending that plaintiffs "persistently confuse  
11 speculative allegations and untested assertions for established  
12 facts," the government attacks the Klein and Marcus declarations  
13 and the various media reports that plaintiffs rely on to  
14 demonstrate standing. Id at 4. The government also argues that  
15 "[e]ven when alleged facts have been the 'subject of widespread  
16 media and public speculation' based on '[u]nofficial leaks and  
17 public surmise,' those alleged facts are not actually established  
18 in the public domain." Id at 8 (quoting Afshar v Dept of State,  
19 702 F2d 1125, 1130-31 (DC Cir 1983)).

20 The government further contends that its "privilege  
21 assertion covers any information tending to confirm or deny (a) the  
22 alleged intelligence activities, (b) whether AT&T was involved with  
23 any such activity, and (c) whether a particular individual's  
24 communications were intercepted as a result of any such activity."  
25 Gov MTD at 17-18. The government reasons that "[w]ithout these  
26 facts \* \* \* [p]laintiffs ultimately will not be able to prove  
27 injury-in-fact and causation," thereby justifying dismissal of this  
28 action for lack of standing. Id at 18.



1           The government also notes that plaintiffs do not fall  
2 within the scope of the publicly disclosed "terrorist surveillance  
3 program" (see *infra* I(C)(1)) because "[p]laintiffs do not claim to  
4 be, or to communicate with, members or affiliates of [the] al Qaeda  
5 [terrorist organization] -- indeed, [p]laintiffs expressly exclude  
6 from their purported class any foreign powers or agent of foreign  
7 powers \* \* \*." *Id* at 18 n9 (citing FAC, ¶ 70). Hence, the  
8 government concludes the named plaintiffs "are in no different  
9 position from any other citizen or AT&T subscriber who falls  
10 outside the narrow scope of the [terrorist surveillance program]  
11 but nonetheless disagrees with the program." *Id* (emphasis in  
12 original).

13           Additionally, the government contends that plaintiffs'  
14 Fourth Amendment claim fails because no warrant is required for the  
15 alleged searches. In particular, the government contends that the  
16 executive has inherent constitutional authority to conduct  
17 warrantless searches for foreign intelligence purposes, *id* at 24  
18 (citing *In re Sealed Case*, 310 F3d 717, 742 (For Intel Surv Ct of  
19 Rev 2002)), and that the warrant requirement does not apply here  
20 because this case involves "special needs" that go beyond a routine  
21 interest in law enforcement, *id* at 26. Accordingly, to make a  
22 *prima facie* case, the government asserts that plaintiffs would have  
23 to demonstrate that the alleged searches were unreasonable, which  
24 would require a fact-intensive inquiry that the government contends  
25 plaintiffs could not perform because of the asserted privilege. *Id*  
26 at 26-27.

27 //

28 //

1           The government also argues that plaintiffs cannot  
2 establish a *prima facie* case for their statutory claims because  
3 plaintiffs must prove "that any alleged interception or disclosure  
4 was not authorized by the Government." The government maintains  
5 that "[p]laintiffs bear the burden of alleging and proving the lack  
6 of such authorization," *id* at 21-22, and that they cannot meet that  
7 burden because "information confirming or denying AT&T's  
8 involvement in alleged intelligence activities is covered by the  
9 state secrets assertion." *Id* at 23.

10           Because "the existence or non-existence of any  
11 certification or authorization by the Government relating to any  
12 AT&T activity would be information tending to confirm or deny  
13 AT&T's involvement in any alleged intelligence activity," Doc #145-  
14 1 (Gov 5/17/06 Br) at 17, the government contends that its state  
15 secrets assertion precludes AT&T from "present[ing] the facts that  
16 would constitute its defenses." Gov Reply at 1. Accordingly, the  
17 government also argues that the court could grant summary judgment  
18 in favor of AT&T on that basis.

19  
20           C

21           The first step in determining whether a piece of  
22 information constitutes a "state secret" is determining whether  
23 that information actually is a "secret." Hence, before analyzing  
24 the application of the state secrets privilege to plaintiffs'  
25 claims, the court summarizes what has been publicly disclosed about  
26 NSA surveillance programs as well as the AT&T documents and  
27 accompanying Klein and Marcus declarations.

28 //

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

1

Within the last year, public reports have surfaced on at least two different types of alleged NSA surveillance programs, neither of which relies on warrants. The New York Times disclosed the first such program on December 16, 2005. Doc #19 (Cohn Decl), Ex J (James Risen and Eric Lichtblau, *Bush Lets US Spy on Callers Without Courts*, The New York Times (Dec 16, 2005)). The following day, President George W Bush confirmed the existence of a "terrorist surveillance program" in his weekly radio address:

In the weeks following the [September 11, 2001] terrorist attacks on our Nation, I authorized the National Security Agency, consistent with US law and the Constitution, to intercept the international communications of people with known links to Al Qaeda and related terrorist organizations. Before we intercept these communications, the Government must have information that establishes a clear link to these terrorist networks.

Doc #20 (Pl Request for Judicial Notice), Ex 1 at 2, available at <http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html> (last visited July 19, 2006). The President also described the mechanism by which the program is authorized and reviewed:

The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our Government and the threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our Nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for as long as our Nation faces a continuing threat from Al Qaeda and related groups.

//  
//

1 The NSA's activities under this authorization are  
2 thoroughly reviewed by the Justice Department and  
3 NSA's top legal officials, including NSA's General  
4 Counsel and Inspector General. Leaders in Congress  
5 have been briefed more than a dozen times on this  
6 authorization and the activities conducted under  
7 it. Intelligence officials involved in this  
8 activity also receive extensive training to ensure  
9 they perform their duties consistent with the  
10 letter and intent of the authorization.

11 Id.

12 Attorney General Alberto Gonzales subsequently confirmed  
13 that this program intercepts "contents of communications where \* \* \*  
14 one party to the communication is outside the United States" and  
15 the government has "a reasonable basis to conclude that one party  
16 to the communication is a member of al Qaeda, affiliated with al  
17 Qaeda, or a member of an organization affiliated with al Qaeda, or  
18 working in support of al Qaeda." Doc #87 (AT&T Request for  
19 Judicial Notice), Ex J at 1 (hereinafter "12/19/05 Press  
20 Briefing"), available at [http://www.whitehouse.gov/news/releases/  
21 2005/12/print/20051219-1.html](http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html) (last visited July 19, 2005). The  
22 Attorney General also noted, "This [program] is not about  
23 wiretapping everyone. This is a very concentrated, very limited  
24 program focused at gaining information about our enemy." Id at 5.  
25 The President has also made a public statement, of which the court  
26 takes judicial notice, that the government's "international  
27 activities strictly target al Qaeda and their known affiliates,"  
28 "the government does not listen to domestic phone calls without  
court approval" and the government is "not mining or trolling  
through the personal lives of millions of innocent Americans." The  
White House, *President Bush Discusses NSA Surveillance Program* (May  
11, 2006) (hereinafter "5/11/06 Statement"), [http://www.whitehouse.](http://www.whitehouse)

1 gov/news/releases/2006/05/20060511-1.html (last visited July 19,  
2 2005).

3           On May 11, 2006, USA Today reported the existence of a  
4 second NSA program in which BellSouth Corp, Verizon Communications  
5 Inc and AT&T were alleged to have provided telephone calling  
6 records of tens of millions of Americans to the NSA. Doc #182  
7 (Markman Decl), Ex 5 at 1 (Leslie Cauley, *NSA Has Massive Database*  
8 *of Americans' Phone Calls*, USA Today (May 11, 2006)). The article  
9 did not allege that the NSA listens to or records conversations but  
10 rather that BellSouth, Verizon and AT&T gave the government access  
11 to a database of domestic communication records that the NSA uses  
12 "to analyze calling patterns in an effort to detect terrorist  
13 activity." Id. The report indicated a fourth telecommunications  
14 company, Qwest Communications International Inc, declined to  
15 participate in the program. Id at 2. An attorney for Qwest's  
16 former CEO, Joseph Nacchio, issued the following statement:

17           In the Fall of 2001 \* \* \* while Mr Nacchio was  
18 Chairman and CEO of Qwest and was serving pursuant  
19 to the President's appointment as the Chairman of  
20 the National Security Telecommunications Advisory  
Committee, Qwest was approached to permit the  
Government access to the private telephone records  
of Qwest customers.

21           Mr Nacchio made inquiry as to whether a warrant or  
22 other legal process had been secured in support of  
23 that request. When he learned that no such  
24 authority had been granted and that there was a  
25 disinclination on the part of the authorities to  
26 use any legal process, including the Special Court  
27 which had been established to handle such matters,  
28 Mr Nacchio concluded that these requests violated  
the privacy requirements of the Telecommunications  
[sic] Act. Accordingly, Mr Nacchio issued  
instructions to refuse to comply with these  
requests. These requests continued throughout Mr  
Nacchio's tenure and until his departure in June of  
2002.

1 Markman Decl, Ex 6.

2 BellSouth and Verizon both issued statements, of which  
3 the court takes judicial notice, denying their involvement in the  
4 program described in USA Today. BellSouth stated in relevant part:

5 As a result of media reports that BellSouth  
6 provided massive amounts of customer calling  
7 information under a contract with the NSA, the  
8 Company conducted an internal review to determine  
9 the facts. Based on our review to date, we have  
10 confirmed no such contract exists and we have not  
11 provided bulk customer calling records to the NSA.

12 News Release, BellSouth Statement on Governmental Data Collection  
13 (May 15, 2006), available at [http://bellsouth.mediaroom.com/](http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860)  
14 [index.php?s=press\\_releases&item=2860](http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860) (last visited July 19, 2006).

15 Although declining to confirm or deny whether it had any  
16 relationship to the NSA program acknowledged by the President,  
17 Verizon stated in relevant part:

18 One of the most glaring and repeated falsehoods in  
19 the media reporting is the assertion that, in the  
20 aftermath of the 9/11 attacks, Verizon was  
21 approached by NSA and entered into an arrangement  
22 to provide the NSA with data from its customers'  
23 domestic calls.

24 This is false. From the time of the 9/11 attacks  
25 until just four months ago, Verizon had three major  
26 businesses - its wireline phone business, its  
27 wireless company and its directory publishing  
28 business. It also had its own Internet Service  
29 Provider and long-distance businesses. Contrary to  
30 the media reports, Verizon was not asked by NSA to  
31 provide, nor did Verizon provide, customer phone  
32 records from any of these businesses, or any call  
33 data from those records. None of these companies  
34 -- wireless or wireline -- provided customer  
35 records or call data.

36 See News Release, Verizon Issues Statement on NSA Media Coverage  
37 (May 16, 2006), available at [http://newscenter.verizon.com/](http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450)  
38 [proactive/newsroom/release.vtml?id=93450](http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450) (last visited July 19,  
2006). BellSouth and Verizon's denials have been at least somewhat

1 substantiated in later reports. Doc #298 (DiMuzio Decl), Ex 1  
2 (*Lawmakers: NSA Database Incomplete*, USA Today (June 30, 2006)).  
3 Neither AT&T nor the government has confirmed or denied the  
4 existence of a program of providing telephone calling records to  
5 the NSA. Id.

6  
7 2

8 Although the government does not claim that the AT&T  
9 documents obtained by Mark Klein or the accompanying declarations  
10 contain classified information (Doc #284 (6/23/06 Transcript) at  
11 76:9-20), those papers remain under seal because AT&T alleges that  
12 they contain proprietary and trade secret information.  
13 Nonetheless, much of the information in these papers has already  
14 been leaked to the public or has been revealed in redacted versions  
15 of the papers. The summary below is based on those already  
16 disclosed facts.

17 In a public statement, Klein explained that while working  
18 at an AT&T office in San Francisco in 2002, "the site manager told  
19 me to expect a visit from a National Security Agency agent, who was  
20 to interview a management-level technician for a special job." Doc  
21 #43 (Ericson Decl), Ex J at 1. While touring the Folsom Street  
22 AT&T facility in January 2003, Klein "saw a new room being built  
23 adjacent to the 4ESS switch room where the public's phone calls are  
24 routed" and "learned that the person whom the NSA interviewed for  
25 the secret job was the person working to install equipment in this  
26 room." Id. See also Doc #147 (Redact Klein Decl), ¶ 10 ("The NSA  
27 agent came and met with [Field Support Specialist (FSS)] #2. FSS  
28 #1 later confirmed to me that FSS #2 was working on the special

1 job."); id, ¶ 16 ("In the Fall of 2003, FSS #1 told me that another  
2 NSA agent would again visit our office \* \* \* to talk to FSS #1 in  
3 order to get the latter's evaluation of FSS #3's suitability to  
4 perform the special job that FSS #2 had been doing. The NSA agent  
5 did come and speak to FSS #1.").

6 Klein then learned about the AT&T documents in October  
7 2003, after being transferred to the Folsom Street facility to  
8 oversee the Worldnet Internet room. Ericson Decl, Ex J at 2. One  
9 document described how "fiber optic cables from the secret room  
10 were tapping into the Worldnet circuits by splitting off a portion  
11 of the light signal." Id. The other two documents "instructed  
12 technicians on connecting some of the already in-service circuits  
13 to [a] 'splitter' cabinet, which diverts some of the light signal  
14 to the secret room." Id. Klein noted the secret room contained "a  
15 Narus STA 6400" and that "Narus STA technology is known to be used  
16 particularly by government intelligence agencies because of its  
17 ability to sift through large amounts of data looking for  
18 preprogrammed targets." Id. Klein also "learned that other such  
19 'splitter' cabinets were being installed in other cities, including  
20 Seattle, San Jose, Los Angeles and San Diego." Id.

21  
22 D

23 Based on the foregoing, it might appear that none of the  
24 subject matter in this litigation could be considered a secret  
25 given that the alleged surveillance programs have been so widely  
26 reported in the media.

27 //

28 //



1           The court recognizes, however, that simply because a  
2 factual statement has been publicly made does not necessarily mean  
3 that the facts it relates are true and are not a secret. The  
4 statement also must come from a reliable source. Indeed, given the  
5 sheer amount of statements that have been made in the public sphere  
6 about the alleged surveillance programs and the limited number of  
7 permutations that such programs could take, it would seem likely  
8 that the truth about these programs has already been publicly  
9 reported somewhere. But simply because such statements have been  
10 publicly made does not mean that the truth of those statements is a  
11 matter of general public knowledge and that verification of the  
12 statement is harmless.

13           In determining whether a factual statement is a secret  
14 for purposes of the state secrets privilege, the court should look  
15 only at publicly reported information that possesses substantial  
16 indicia of reliability and whose verification or substantiation  
17 possesses the potential to endanger national security. That  
18 entails assessing the value of the information to an individual or  
19 group bent on threatening the security of the country, as well as  
20 the secrecy of the information.

21           For instance, if this litigation verifies that AT&T  
22 assists the government in monitoring communication records, a  
23 terrorist might well cease using AT&T and switch to other, less  
24 detectable forms of communication. Alternatively, if this  
25 litigation reveals that the communication records program does not  
26 exist, then a terrorist who had been avoiding AT&T might start  
27 using AT&T if it is a more efficient form of communication. In  
28 short, when deciding what communications channel to use, a

1 terrorist "balanc[es] the risk that a particular method of  
2 communication will be intercepted against the operational  
3 inefficiencies of having to use ever more elaborate ways to  
4 circumvent what he thinks may be intercepted." 6/23/06 Transcript  
5 at 48:14-17 (government attorney). A terrorist who operates with  
6 full information is able to communicate more securely and more  
7 efficiently than a terrorist who operates in an atmosphere of  
8 uncertainty.

9 It is, of course, an open question whether individuals  
10 inclined to commit acts threatening the national security engage in  
11 such calculations. But the court is hardly in a position to  
12 second-guess the government's assertions on this matter or to  
13 estimate the risk tolerances of terrorists in making their  
14 communications and hence at this point in the litigation eschews  
15 the attempt to weigh the value of the information.

16 Accordingly, in determining whether a factual statement  
17 is a secret, the court considers only public admissions or denials  
18 by the government, AT&T and other telecommunications companies,  
19 which are the parties indisputably situated to disclose whether and  
20 to what extent the alleged programs exist. In determining what is  
21 a secret, the court at present refrains from relying on the  
22 declaration of Mark Klein. Although AT&T does not dispute that  
23 Klein was a former AT&T technician and he has publicly declared  
24 under oath that he observed AT&T assisting the NSA in some capacity  
25 and his assertions would appear admissible in connection with the  
26 present motions, the inferences Klein draws have been disputed. To  
27 accept the Klein declaration at this juncture in connection with  
28 the state secrets issue would invite attempts to undermine the

1 privilege by mere assertions of knowledge by an interested party.  
2 Needless to say, this does not reflect that the court discounts  
3 Klein's credibility, but simply that what is or is not secret  
4 depends on what the government and its alleged operative AT&T and  
5 other telecommunications providers have either admitted or denied  
6 or is beyond reasonable dispute.

7           Likewise, the court does not rely on media reports about  
8 the alleged NSA programs because their reliability is unclear. To  
9 illustrate, after Verizon and BellSouth denied involvement in the  
10 program described in USA Today in which communication records are  
11 monitored, USA Today published a subsequent story somewhat backing  
12 down from its earlier statements and at least in some measure  
13 substantiating these companies' denials. See *supra* I(C)(1).

14           Finally, the court notes in determining whether the  
15 privilege applies, the court is not limited to considering strictly  
16 admissible evidence. FRE 104(a) ("Preliminary questions concerning  
17 \* \* \* the existence of a privilege \* \* \* shall be determined by the  
18 court, subject to the provisions of subdivision (b). In making its  
19 determination it is not bound by the rules of evidence except those  
20 with respect to privileges."). This makes sense: the issue at bar  
21 is not proving a question of liability but rather determining  
22 whether information that the government contends is a secret is  
23 actually a secret. In making this determination, the court may  
24 rely upon reliable public evidence that might otherwise be  
25 inadmissible at trial because it does not comply with the technical  
26 requirements of the rules of evidence.

27           With these considerations in mind, the court at last  
28 determines whether the state secrets privilege applies here.

E

1  
2 Because this case involves an alleged covert relationship  
3 between the government and AT&T, the court first determines whether  
4 to apply the categorical bar to suit established by the Supreme  
5 Court in Totten v United States, 92 US 105 (1875), acknowledged in  
6 United States v Reynolds, 345 US 1 (1953) and Kasza v Browner, 133  
7 F3d 1159 (9th Cir 1998), and reaffirmed in Tenet v Doe, 544 US 1  
8 (2005). See *id* at 6 (“[A]pplication of the Totten rule of  
9 dismissal \* \* \* represents the sort of ‘threshold question’ we have  
10 recognized may be resolved before addressing jurisdiction.”). The  
11 court then examines the closely related questions whether this  
12 action must be presently dismissed because “the very subject matter  
13 of the action” is a state secret or because the state secrets  
14 privilege necessarily blocks evidence essential to plaintiffs’  
15 *prima facie* case or AT&T’s defense. See Kasza, 133 F3d at 1166-67.

1

16  
17  
18 Although the principles announced in Totten, Tenet,  
19 Reynolds and Kasza inform the court’s decision here, those cases  
20 are not strictly analogous to the facts at bar.

21 First, the instant plaintiffs were not a party to the  
22 alleged covert arrangement at issue here between AT&T and the  
23 government. Hence, Totten and Tenet are not on point to the extent  
24 they hold that former spies cannot enforce agreements with the  
25 government because the parties implicitly agreed that such suits  
26 would be barred. The implicit notion in Totten was one of  
27 equitable estoppel: one who agrees to conduct covert operations  
28 impliedly agrees not to reveal the agreement even if the agreement

1 is breached. But AT&T, the alleged spy, is not the plaintiff here.  
2 In this case, plaintiffs made no agreement with the government and  
3 are not bound by any implied covenant of secrecy.

4 More importantly, unlike the clandestine spy arrangements  
5 in Tenet and Totten, AT&T and the government have for all practical  
6 purposes already disclosed that AT&T assists the government in  
7 monitoring communication content. As noted earlier, the government  
8 has publicly admitted the existence of a "terrorist surveillance  
9 program," which the government insists is completely legal. This  
10 program operates without warrants and targets "contents of  
11 communications where \* \* \* one party to the communication is  
12 outside the United States" and the government has "a reasonable  
13 basis to conclude that one party to the communication is a member  
14 of al Qaeda, affiliated with al Qaeda, or a member of an  
15 organization affiliated with al Qaeda, or working in support of al  
16 Qaeda." 12/19/05 Press Briefing at 1.

17 Given that the "terrorist surveillance program" tracks  
18 "calls into the United States or out of the United States," 5/11/06  
19 Statement, it is inconceivable that this program could exist  
20 without the acquiescence and cooperation of some telecommunications  
21 provider. Although of record here only in plaintiffs' pleading, it  
22 is beyond reasonable dispute that "prior to its being acquired by  
23 SBC, AT&T Corp was the second largest Internet provider in the  
24 country," FAC, ¶ 26, and "AT&T Corp's bundled local and long  
25 distance service was available in 46 states, covering more than 73  
26 million households," id, ¶ 25. AT&T's assistance would greatly  
27 help the government implement this program. See also id, ¶ 27  
28 ("The new AT&T Inc constitutes the largest telecommunications

1 provider in the United States and one of the largest in the  
2 world.""). Considering the ubiquity of AT&T telecommunications  
3 services, it is unclear whether this program could even exist  
4 without AT&T's acquiescence and cooperation.

5           Moreover, AT&T's history of cooperating with the  
6 government on such matters is well known. AT&T has recently  
7 disclosed that it "performs various classified contracts, and  
8 thousands of its employees hold government security clearances."  
9 FAC, ¶ 29. More recently, in response to reports on the alleged  
10 NSA programs, AT&T has disclosed in various statements, of which  
11 the court takes judicial notice, that it has "an obligation to  
12 assist law enforcement and other government agencies responsible  
13 for protecting the public welfare, whether it be an individual or  
14 the security interests of the entire nation. \* \* \* If and when  
15 AT&T is asked to help, we do so strictly within the law and under  
16 the most stringent conditions." News Release, AT&T Statement on  
17 Privacy and Legal/Security Issues (May 11, 2006) (emphasis added),  
18 available at [http://www.sbc.com/gen/press-room?pid=4800&cdvn=news](http://www.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22285)  
19 [&newsarticleid=22285](http://www.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22285). See also Declan McCullagh, CNET News.com,  
20 Legal Loophole Emerges in NSA Spy Program (May 19, 2006) ("Mark  
21 Bien, a spokesman for AT&T, told CNET News.com on Wednesday:  
22 'Without commenting on or confirming the existence of the program,  
23 we can say that when the government asks for our help in protecting  
24 national security, and the request is within the law, we will  
25 provide that assistance.'"), available at [http://news.com.com/](http://news.com.com/Legal+loophole+emerges+in+NSA+spy+program/2100-1028_3-6073600.html)  
26 [Legal+loophole+emerges+in+NSA+spy+program/2100-1028\\_3-6073600.html](http://news.com.com/Legal+loophole+emerges+in+NSA+spy+program/2100-1028_3-6073600.html);  
27 Justin Scheck, Plaintiffs Can Keep AT&T Papers in Domestic Spying  
28 Case, The Recorder (May 18, 2006) ("Marc Bien, a spokesman for

1 AT&T, said he didn't see a settlement on the horizon. 'When the  
2 government asks for our help in protecting American security, and  
3 the request is within the law, we provide assistance,' he said."),  
4 available at <http://www.law.com/jsp/article.jsp?id=1147856734796>.  
5 And AT&T at least presently believes that any such assistance would  
6 be legal if AT&T were simply a passive agent of the government or  
7 if AT&T received a government certification authorizing the  
8 assistance. 6/23/06 Transcript at 15:11-21:19. Hence, it appears  
9 AT&T helps the government in classified matters when asked and AT&T  
10 at least currently believes, on the facts as alleged in plaintiffs'  
11 complaint, its assistance is legal.

12 In sum, the government has disclosed the general contours  
13 of the "terrorist surveillance program," which requires the  
14 assistance of a telecommunications provider, and AT&T claims that  
15 it lawfully and dutifully assists the government in classified  
16 matters when asked.

17 A remaining question is whether, in implementing the  
18 "terrorist surveillance program," the government ever requested the  
19 assistance of AT&T, described in these proceedings as the mother of  
20 telecommunications "that in a very literal way goes all the way  
21 back to Alexander Graham Bell summoning his assistant Watson into  
22 the room." Id at 102:11-13. AT&T's assistance in national  
23 security surveillance is hardly the kind of "secret" that the  
24 Totten bar and the state secrets privilege were intended to protect  
25 or that a potential terrorist would fail to anticipate.

26 //  
27 //  
28 //





1           The court does not "balanc[e the] ultimate interests at  
2 stake in the litigation." Halkin II, 690 F2d at 990. But no case  
3 dismissed because its "very subject matter" was a state secret  
4 involved ongoing, widespread violations of individual  
5 constitutional rights, as plaintiffs allege here. Indeed, most  
6 cases in which the "very subject matter" was a state secret  
7 involved classified details about either a highly technical  
8 invention or a covert espionage relationship. See, e g, Sterling v  
9 Tenet, 416 F3d 338, 348 (4th Cir 2005) (dismissing Title VII racial  
10 discrimination claim that "center[ed] around a covert agent's  
11 assignments, evaluations, and colleagues"); Kasza, 133 F3d at 1162-  
12 63, 1170 (dismissing RCRA claim regarding facility reporting and  
13 inventory requirements at a classified Air Force location near  
14 Groom Lake, Nevada); Zuckerbraun v General Dynamics Corp, 935 F2d  
15 544, 547-48 (2d Cir 1991) (dismissing wrongful death claim  
16 implicating classified information about the "design, manufacture,  
17 performance, functional characteristics, and testing of [weapons]  
18 systems and the rules of engagement"); Fitzgerald v Penthouse Intl,  
19 776 F2d 1236, 1242-43 (4th Cir 1985) (dismissing libel suit  
20 "charging the plaintiff with the unauthorized sale of a top secret  
21 marine mammal weapons system"); Halpern v United States, 258 F2d  
22 36, 44 (2d Cir 1958) (rejecting government's motion to dismiss in a  
23 case involving a patent with military applications withheld under a  
24 secrecy order); Clift v United States, 808 F Supp 101, 111 (D Conn  
25 1991) (dismissing patent dispute over a cryptographic encoding  
26 device).

27 //

28 //

1 By contrast, the very subject matter of this action is  
2 hardly a secret. As described above, public disclosures by the  
3 government and AT&T indicate that AT&T is assisting the government  
4 to implement some kind of surveillance program. See *supra* I(E)(1).

5 For this reason, the present action is also different  
6 from El-Masri v Tenet, the recently dismissed case challenging the  
7 government's alleged "extraordinary rendition program." In El-  
8 Masri, only limited sketches of the alleged program had been  
9 disclosed and the whole object of the suit was to reveal classified  
10 details regarding "the means and methods the foreign intelligence  
11 services of this and other countries used to carry out the  
12 program." El-Masri, 2006 WL 1391390, \*5. By contrast, this case  
13 focuses only on whether AT&T intercepted and disclosed  
14 communications or communication records to the government. And as  
15 described above, significant amounts of information about the  
16 government's monitoring of communication content and AT&T's  
17 intelligence relationship with the government are already non-  
18 classified or in the public record.

19  
20 3

21 The court also declines to decide at this time whether  
22 this case should be dismissed on the ground that the government's  
23 state secrets assertion will preclude evidence necessary for  
24 plaintiffs to establish a *prima facie* case or for AT&T to raise a  
25 valid defense to the claims. Plaintiffs appear to be entitled to  
26 at least some discovery. See *infra* I(G)(3). It would be premature  
27 to decide these issues at the present time. In drawing this  
28 conclusion, the court is following the approach of the courts in

1 Halkin v Helms and Ellsberg v Mitchell; these courts did not  
2 dismiss those cases at the outset but allowed them to proceed to  
3 discovery sufficiently to assess the state secrets privilege in  
4 light of the facts. The government has not shown why that should  
5 not be the course of this litigation.

6  
7 4

8 In sum, for much the same reasons that Totten does not  
9 preclude this suit, the very subject matter of this action is not a  
10 "secret" for purposes of the state secrets privilege and it would  
11 be premature to conclude that the privilege will bar evidence  
12 necessary for plaintiffs' *prima facie* case or AT&T's defense.  
13 Because of the public disclosures by the government and AT&T, the  
14 court cannot conclude that merely maintaining this action creates a  
15 "reasonable danger" of harming national security. Accordingly,  
16 based on the foregoing, the court DENIES the government's motion to  
17 dismiss.

18  
19 F

20 The court hastens to add that its present ruling should  
21 not suggest that its *in camera*, *ex parte* review of the classified  
22 documents confirms the truth of the particular allegations in  
23 plaintiffs' complaint. Plaintiffs allege a surveillance program of  
24 far greater scope than the publicly disclosed "terrorist  
25 surveillance program." The existence of this alleged program and  
26 AT&T's involvement, if any, remain far from clear. And as in  
27 Halkin v Helms, it is certainly possible that AT&T might be  
28 entitled to summary judgment at some point if the court finds that

1 the state secrets privilege blocks certain items of evidence that  
2 are essential to plaintiffs' *prima facie* case or AT&T's defense.  
3 The court also recognizes that legislative or other developments  
4 might alter the course of this litigation.

5           But it is important to note that even the state secrets  
6 privilege has its limits. While the court recognizes and respects  
7 the executive's constitutional duty to protect the nation from  
8 threats, the court also takes seriously its constitutional duty to  
9 adjudicate the disputes that come before it. See Hamdi v Rumsfeld,  
10 542 US 507, 536 (2004) (plurality opinion) ("Whatever power the  
11 United States Constitution envisions for the Executive in its  
12 exchanges with other nations or with enemy organizations in times  
13 of conflict, it most assuredly envisions a role for all three  
14 branches when individual liberties are at stake."). To defer to a  
15 blanket assertion of secrecy here would be to abdicate that duty,  
16 particularly because the very subject matter of this litigation has  
17 been so publicly aired. The compromise between liberty and  
18 security remains a difficult one. But dismissing this case at the  
19 outset would sacrifice liberty for no apparent enhancement of  
20 security.

21 //  
22 //  
23 //  
24 //  
25 //  
26 //  
27 //  
28 //

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

G

The government also contends the issue whether AT&T received a certification authorizing its assistance to the government is a state secret. Gov 5/17/06 Br at 17.

1

The procedural requirements and impact of a certification under Title III are addressed in 18 USC § 2511(2)(a)(ii):

Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, \* \* \* are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of [FISA] \* \* \* if such provider, its officers, employees, or agents, \* \* \* has been provided with -- \* \* \*

(B) a certification in writing by a person specified in section 2518(7) of this title [18 USCS § 2518(7)] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required \* \* \*.

Although it is doubtful whether plaintiffs' constitutional claim would be barred by a valid certification under section 2511(2)(a)(ii), this provision on its face makes clear that a valid certification would preclude the statutory claims asserted here. See 18 USC § 2511(2)(a)(ii) ("No cause of action shall lie in any court against any provider of wire or electronic communication service \* \* \* for providing information, facilities, or assistance in accordance with the terms of a \* \* \* certification under this chapter.").

//

2

As noted above, it is not a secret for purposes of the state secrets privilege that AT&T and the government have some kind of intelligence relationship. See *supra* I(E)(1). Nonetheless, the court recognizes that uncovering whether and to what extent a certification exists might reveal information about AT&T's assistance to the government that has not been publicly disclosed. Accordingly, in applying the state secrets privilege to the certification question, the court must look deeper at what information has been publicly revealed about the alleged electronic surveillance programs. The following chart summarizes what the government has disclosed about the scope of these programs in terms of (1) the individuals whose communications are being monitored, (2) the locations of those individuals and (3) the types of information being monitored:

	Purely domestic communication content	Domestic-foreign communication content	Communication records
General public	Government DENIES	Government DENIES	Government NEITHER CONFIRMS NOR DENIES
al Qaeda or affiliate member/agent	Government DENIES	Government CONFIRMS	

As the chart relates, the government's public disclosures regarding monitoring of "communication content" (i e, wiretapping or listening in on a communication) differ significantly from its disclosures regarding "communication records" (i e, collecting ancillary data pertaining to a communication, such as the telephone

1 numbers dialed by an individual). See *supra* I(C)(1). Accordingly,  
2 the court separately addresses for each alleged program whether  
3 revealing the existence or scope of a certification would disclose  
4 a state secret.

5  
6 3

7 Beginning with the warrantless monitoring of  
8 "communication content," the government has confirmed that it  
9 monitors "contents of communications where \* \* \* one party to the  
10 communication is outside the United States" and the government has  
11 "a reasonable basis to conclude that one party to the communication  
12 is a member of al Qaeda, affiliated with al Qaeda, or a member of  
13 an organization affiliated with al Qaeda, or working in support of  
14 al Qaeda." 12/19/05 Press Briefing at 1. The government denies  
15 listening in without a warrant on any purely domestic  
16 communications or communications in which neither party has a  
17 connection to al Qaeda or a related terrorist organization. In  
18 sum, regarding the government's monitoring of "communication  
19 content," the government has disclosed the universe of  
20 possibilities in terms of whose communications it monitors and  
21 where those communicating parties are located.

22 Based on these public disclosures, the court cannot  
23 conclude that the existence of a certification regarding the  
24 "communication content" program is a state secret. If the  
25 government's public disclosures have been truthful, revealing  
26 whether AT&T has received a certification to assist in monitoring  
27 communication content should not reveal any new information that  
28 would assist a terrorist and adversely affect national security.

1 And if the government has not been truthful, the state secrets  
2 privilege should not serve as a shield for its false public  
3 statements. In short, the government has opened the door for  
4 judicial inquiry by publicly confirming and denying material  
5 information about its monitoring of communication content.

6 Accordingly, the court concludes that the state secrets  
7 privilege will not prevent AT&T from asserting a certification-  
8 based defense, as appropriate, regarding allegations that it  
9 assisted the government in monitoring communication content. The  
10 court envisions that AT&T could confirm or deny the existence of a  
11 certification authorizing monitoring of communication content  
12 through a combination of responses to interrogatories and *in camera*  
13 review by the court. Under this approach, AT&T could reveal  
14 information at the level of generality at which the government has  
15 publicly confirmed or denied its monitoring of communication  
16 content. This approach would also enable AT&T to disclose the non-  
17 privileged information described here while withholding any  
18 incidental privileged information that a certification might  
19 contain.

20  
21 4

22 Turning to the alleged monitoring of communication  
23 records, the court notes that despite many public reports on the  
24 matter, the government has neither confirmed nor denied whether it  
25 monitors communication records and has never publicly disclosed  
26 whether the NSA program reported by USA Today on May 11, 2006,  
27 actually exists. Although BellSouth, Verizon and Qwest have denied  
28 participating in this program, AT&T has neither confirmed nor



1 denied its involvement. Hence, unlike the program monitoring  
2 communication content, the general contours and even the existence  
3 of the alleged communication records program remain unclear.

4 Nonetheless, the court is hesitant to conclude that the  
5 existence or non-existence of the communication records program  
6 necessarily constitutes a state secret. Confirming or denying the  
7 existence of this program would only affect a terrorist who was  
8 insensitive to the publicly disclosed "terrorist surveillance  
9 program" but cared about the alleged program here. This would seem  
10 unlikely to occur in practice given that the alleged communication  
11 records program, which does not involve listening in on  
12 communications, seems less intrusive than the "terrorist  
13 surveillance program," which involves wiretapping. And in any  
14 event, it seems odd that a terrorist would continue using AT&T  
15 given that BellSouth, Verizon and Qwest have publicly denied  
16 participating in the alleged communication records program and  
17 would appear to be safer choices. Importantly, the public denials  
18 by these telecommunications companies undercut the government and  
19 AT&T's contention that revealing AT&T's involvement or lack thereof  
20 in the program would disclose a state secret.

21 Still, the court recognizes that it is not in a position  
22 to estimate a terrorist's risk preferences, which might depend on  
23 facts not before the court. For example, it may be that a  
24 terrorist is unable to avoid AT&T by choosing another provider or,  
25 for reasons outside his control, his communications might  
26 necessarily be routed through an AT&T facility. Revealing that a  
27 communication records program exists might encourage that terrorist  
28 to switch to less efficient but less detectable forms of

1 communication. And revealing that such a program does not exist  
2 might encourage a terrorist to use AT&T services when he would not  
3 have done so otherwise. Accordingly, for present purposes, the  
4 court does not require AT&T to disclose what relationship, if any,  
5 it has with this alleged program.

6 The court stresses that it does not presently conclude  
7 that the state secrets privilege will necessarily preclude AT&T  
8 from revealing later in this litigation information about the  
9 alleged communication records program. While this case has been  
10 pending, the government and telecommunications companies have made  
11 substantial public disclosures on the alleged NSA programs. It is  
12 conceivable that these entities might disclose, either deliberately  
13 or accidentally, other pertinent information about the  
14 communication records program as this litigation proceeds. The  
15 court recognizes such disclosures might make this program's  
16 existence or non-existence no longer a secret. Accordingly, while  
17 the court presently declines to permit any discovery regarding the  
18 alleged communication records program, if appropriate, plaintiffs  
19 can request that the court revisit this issue in the future.

20

21

5

22

23

24

25

26

27

28

Finally, the court notes plaintiffs contend that Congress, through various statutes, has limited the state secrets privilege in the context of electronic surveillance and has abrogated the privilege regarding the existence of a government certification. See Doc #192 (Pl Opp Gov MTD) at 16-26, 45-48. Because these arguments potentially implicate highly complicated separation of powers issues regarding Congress' ability to abrogate

1 what the government contends is a constitutionally protected  
2 privilege, the court declines to address these issues presently,  
3 particularly because the issues might very well be obviated by  
4 future public disclosures by the government and AT&T. If  
5 necessary, the court may revisit these arguments at a later stage  
6 of this litigation.

7  
8

H

9 The government also asserts two statutory privileges in  
10 its motion to dismiss that it contends apply "to any intelligence-  
11 related information, sources and methods implicated by  
12 [p]laintiffs' claims and the information covered by these privilege  
13 claims are at least co-extensive with the assertion of the state  
14 secrets privilege by the DNI." Gov MTD at 14. First, the  
15 government relies on 50 USC § 402 note, which provides:

16 [N]othing in this Act or any other law \* \* \* shall  
17 be construed to require the disclosure of the  
18 organization or any function of the National  
19 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.

20 The government also relies on 50 USC § 403-1(i)(1), which states,  
21 "The Director of National Intelligence shall protect intelligence  
22 sources and methods from unauthorized disclosure."

23 Neither of these provisions by their terms requires the  
24 court to dismiss this action and it would be premature for the  
25 court to do so at this time. In opposing a subsequent summary  
26 judgment motion, plaintiffs could rely on many non-classified  
27 materials including present and future public disclosures of the  
28 government or AT&T on the alleged NSA programs, the AT&T documents

1 and the supporting Klein and Marcus declarations and information  
2 gathered during discovery. Hence, it is at least conceivable that  
3 some of plaintiffs' claims, particularly with respect to  
4 declaratory and injunctive relief, could survive summary judgment.  
5 After discovery begins, the court will determine step-by-step  
6 whether the privileges prevent plaintiffs from discovering  
7 particular evidence. But the mere existence of these privileges  
8 does not justify dismissing this case now.

9           Additionally, neither of these provisions block AT&T from  
10 producing any certification that it received to assist the  
11 government in monitoring communication content, see *supra* I(G)(3).  
12 Because information about this certification would be revealed only  
13 at the same level of generality as the government's public  
14 disclosures, permitting this discovery should not reveal any new  
15 information on the NSA's activities or its intelligence sources or  
16 methods, assuming that the government has been truthful.

17           Accordingly, the court DENIES the government's motion to  
18 dismiss based on the statutory privileges and DENIES the privileges  
19 with respect to any certification that AT&T might have received  
20 authorizing it to monitor communication content.

21 //  
22 //  
23 //  
24 //  
25 //  
26 //  
27 //  
28 //

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

II

AT&T moves to dismiss plaintiffs' complaint on multiple grounds, contending that (1) plaintiffs lack standing, (2) the amended complaint fails to plead affirmatively the absence of immunity from suit and (3) AT&T is entitled to statutory, common law and qualified immunity. Because standing is a threshold jurisdictional question, the court addresses that issue first. See Steel Company v Citizens for a Better Environment, 523 US 83, 94, 102 (1998).

A

"[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III." Lujan v Defenders of Wildlife, 504 US 555, 560 (1992). To establish standing under Article III, a plaintiff must satisfy three elements: (1) "the plaintiff must have suffered an injury in fact -- an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical," (2) "there must be a causal connection between the injury and the conduct complained of" and (3) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id* at 560-61 (internal quotation marks, citations and footnote omitted). A party invoking federal jurisdiction has the burden of establishing its standing to sue. *Id* at 561.

//  
//  
//

1           In the present case, AT&T contends plaintiffs have not  
2 sufficiently alleged injury-in-fact and their complaint relies on  
3 "wholly conclusory" allegations. AT&T MTD at 20-22. According to  
4 AT&T, "Absent some concrete allegation that the government  
5 monitored their communications or records, all plaintiffs really  
6 have is a suggestion that AT&T provided a means by which the  
7 government could have done so had it wished. This is anything but  
8 injury-in-fact." Id at 20 (emphasis in original). AT&T compares  
9 this case to United Presbyterian Church v Reagan, 738 F2d 1375 (DC  
10 Cir 1984) (written by then-Judge Scalia), in which the court found  
11 that plaintiffs' allegations of unlawful surveillance were "too  
12 generalized and nonspecific to support a complaint." Id at 1380.

13           As a preliminary matter, AT&T incorrectly focuses on  
14 whether plaintiffs have pled that the government "monitored  
15 [plaintiffs'] communications or records" or "targeted [plaintiffs]  
16 or their communications." Instead, the proper focus is on AT&T's  
17 actions. Plaintiffs' statutory claims stem from injuries caused  
18 solely by AT&T through its alleged interception, disclosure, use,  
19 divulgence and/or publication of plaintiffs' communications or  
20 communication records. FAC, ¶¶ 93-95, 102-05, 113-14, 121, 128,  
21 135-41. Hence, plaintiffs need not allege any facts regarding the  
22 government's conduct to state these claims.

23           More importantly, for purposes of the present motion to  
24 dismiss, plaintiffs have stated sufficient facts to allege injury-  
25 in-fact for all their claims. "At the pleading stage, general  
26 factual allegations of injury resulting from the defendant's  
27 conduct may suffice, for on a motion to dismiss we 'presume that  
28 general allegations embrace those specific facts that are necessary

1 to support the claim.'" Lujan, 504 US at 561 (quoting Lujan v  
2 National Wildlife Federation, 497 US 871, 889 (1990)). Throughout  
3 the complaint, plaintiffs generally describe the injuries they have  
4 allegedly suffered because of AT&T's illegal conduct and its  
5 collaboration with the government. See, e g, FAC, ¶ 61 ("On  
6 information and belief, AT&T Corp has provided the government with  
7 direct access to the contents of the Hawkeye, Aurora and/or other  
8 databases that it manages using Daytona, including all information,  
9 records, [dialing, routing, addressing and/or signaling  
10 information] and [customer proprietary network information]  
11 pertaining to [p]laintiffs and class members, by providing the  
12 government with copies of the information in the databases and/or  
13 by giving the government access to Daytona's querying capabilities  
14 and/or some other technology enabling the government agents to  
15 search the databases' contents."); id, ¶ 6 ("On information and  
16 belief, AT&T Corp has opened its key telecommunications facilities  
17 and databases to direct access by the NSA and/or other government  
18 agencies, intercepting and disclosing to the government the  
19 contents of its customers' communications as well as detailed  
20 communications records about millions of its customers, including  
21 [p]laintiffs and class members.").

22 By contrast, plaintiffs in United Presbyterian Church  
23 alleged they "ha[d] been informed on numerous occasions" that mail  
24 that they had sent never reached its destination, "ha[d] reason to  
25 believe that, for a long time, [their] officers, employees, and  
26 persons associated with [them had] been subjected to government  
27 surveillance, infiltration and disruption" and "discern[ed] a long-  
28 term pattern of surveillance of [their] members, disruption of

1 their speaking engagements in this country, and attempts at  
2 character assassination." See 738 F2d at 1380 n2. Because these  
3 allegations were more attenuated and less concrete than the  
4 specific injuries alleged here, United Presbyterian Church does not  
5 support dismissing this action.

6 AT&T also contends "[p]laintiffs lack standing to assert  
7 their statutory claims (Counts II-VII) because the FAC alleges no  
8 facts suggesting that their statutory rights have been violated"  
9 and "the FAC alleges nothing to suggest that the named plaintiffs  
10 were themselves subject to surveillance." AT&T MTD at 24-25  
11 (emphasis in original). But AT&T ignores that the gravamen of  
12 plaintiffs' complaint is that AT&T has created a dragnet that  
13 collects the content and records of its customers' communications.  
14 See, e g, FAC, ¶¶ 42-64. The court cannot see how any one  
15 plaintiff will have failed to demonstrate injury-in-fact if that  
16 plaintiff effectively demonstrates that all class members have so  
17 suffered. This case is plainly distinguishable from Halkin II, for  
18 in that case, showing that plaintiffs were on a watchlist was not  
19 tantamount to showing that any particular plaintiff suffered a  
20 surveillance-related injury-in-fact. See Halkin II, 690 F2d at  
21 999-1001. As long as the named plaintiffs were, as they allege,  
22 AT&T customers during the relevant time period (FAC, ¶¶ 13-16), the  
23 alleged dragnet would have imparted a concrete injury on each of  
24 them.

25 //  
26 //  
27 //  
28 //



1           This conclusion is not altered simply because the alleged  
2 injury is widely shared among AT&T customers. In FEC v Akins, 524  
3 US 11 (1998), the Supreme Court explained:

4           Whether styled as a constitutional or prudential  
5 limit on standing, the Court has sometimes  
6 determined that where large numbers of Americans  
7 suffer alike, the political process, rather than  
8 the judicial process, may provide the more  
9 appropriate remedy for a widely shared grievance.

10          [This] kind of judicial language \* \* \* however,  
11 invariably appears in cases where the harm at issue  
12 is not only widely shared, but is also of an  
13 abstract and indefinite nature.

14 Id at 23. The Court continued:

15          [W]here a harm is concrete, though widely shared,  
16 the Court has found "injury in fact." Thus the  
17 fact that a political forum may be more readily  
18 available where an injury is widely shared (while  
19 counseling against, say, interpreting a statute as  
20 conferring standing) does not, by itself,  
21 automatically disqualify an interest for Article  
22 III purposes. Such an interest, where sufficiently  
23 concrete, may count as an "injury in fact."

24 Id at 24.

25          Here, the alleged injury is concrete even though it is  
26 widely shared. Despite AT&T's alleged creation of a dragnet to  
27 intercept all or substantially all of its customers'  
28 communications, this dragnet necessarily inflicts a concrete injury  
that affects each customer in a distinct way, depending on the  
content of that customer's communications and the time that  
customer spends using AT&T services. Indeed, the present situation  
resembles a scenario in which "large numbers of individuals suffer  
the same common-law injury (say, a widespread mass tort)." Id.

//

//

//

1           AT&T also contends that the state secrets privilege bars  
2 plaintiffs from establishing standing. Doc #244 (AT&T Reply) at  
3 16-18. See also Gov MTD 16-20. But as described above, the state  
4 secrets privilege will not prevent plaintiffs from receiving at  
5 least some evidence tending to establish the factual predicate for  
6 the injury-in-fact underlying their claims directed at AT&T's  
7 alleged involvement in the monitoring of communication content.  
8 See *supra* I(G)(3). And the court recognizes that additional facts  
9 might very well be revealed during, but not as a direct consequence  
10 of, this litigation that obviate many of the secrecy concerns  
11 currently at issue regarding the alleged communication records  
12 program. Hence, it is unclear whether the privilege would  
13 necessarily block AT&T from revealing information about its  
14 participation, if any, in that alleged program. See *supra* I(G)(4).  
15 The court further notes that the AT&T documents and the  
16 accompanying Klein and Marcus declarations provide at least some  
17 factual basis for plaintiffs' standing. Accordingly, the court  
18 does not conclude at this juncture that plaintiffs' claims would  
19 necessarily lack the factual support required to withstand a future  
20 jurisdictional challenge based on lack of standing.

21           Because plaintiffs have sufficiently alleged that they  
22 suffered an actual, concrete injury traceable to AT&T and  
23 redressable by this court, the court DENIES AT&T's motion to  
24 dismiss for lack of standing.

25 //

26 //

27 //

28 //

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

B

AT&T also contends that telecommunications providers are immune from suit if they receive a government certification authorizing them to conduct electronic surveillance. AT&T MTD at 5. AT&T argues that plaintiffs have the burden to plead affirmatively that AT&T lacks such a certification and that plaintiffs have failed to do so here, thereby making dismissal appropriate. Id at 10-13.

As discussed above, the procedural requirements for a certification are addressed in 18 USC § 2511(2)(a)(ii)(B). See *supra* I(G)(1). Under section 2511(2)(a)(ii), "No cause of action shall lie in any court against any provider of wire or electronic communication service \* \* \* for providing information, facilities, or assistance in accordance with the terms of a \* \* \* certification under this chapter." This provision is referenced in 18 USC § 2520(a) (emphasis added), which creates a private right of action under Title III:

Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter [18 USCS §§ 2510 et seq] may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

A similar provision exists at 18 USC § 2703(e) (emphasis added):

No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

1           The court recognizes that the language emphasized above  
2 suggests that to state a claim under these statutes, a plaintiff  
3 must affirmatively allege that a telecommunications provider did  
4 not receive a government certification. And out of the many  
5 statutory exceptions in section 2511, only section 2511(2)(a)(ii)  
6 appears in section 2520(a), thereby suggesting that a lack of  
7 certification is an element of a Title III claim whereas the other  
8 exceptions are simply affirmative defenses. As AT&T notes, this  
9 interpretation is at least somewhat supported by the Senate report  
10 accompanying 18 USC § 2520, which states in relevant part:

11           A civil action will not lie [under 18 USC § 2520]  
12 where the requirements of sections 2511(2)(a)(ii) of  
13 title 18 are met. With regard to that exception,  
the Committee intends that the following procedural  
standards will apply:

14           (1) The complaint must allege that a wire or  
15 electronic communications service provider (or  
one of its employees) (a) disclosed the  
16 existence of a wiretap; (b) acted without a  
facially valid court order or certification;  
17 (c) acted beyond the scope of a court order or  
certification or (d) acted on bad faith.  
18 Acting in bad faith would include failing to  
19 read the order or collusion. If the complaint  
fails to make any of these allegations, the  
20 defendant can move to dismiss the complaint for  
failure to state a claim upon which relief can  
be granted.

21 ECPA, S Rep No 99-541, 99th Cong, 2d Sess 26 (1986) (reprinted in  
22 1986 USCCAN 3555, 3580) (emphasis added).

23           Nonetheless, the statutory text does not explicitly  
24 provide for a heightened pleading requirement, which is in essence  
25 what AT&T seeks to impose here. And the court is reluctant to  
26 infer a heightened pleading requirement into the statute given that  
27 in other contexts, Congress has been explicit when it intended to  
28 create such a requirement. See, e g, Private Securities Litigation

1 Reform Act of 1995, § 101, 15 USC § 78u-4(b)(1), (2) (prescribing  
2 heightened pleading standards for securities class actions).

3 In any event, the court need not decide whether  
4 plaintiffs must plead affirmatively the absence of a certification  
5 because the present complaint, liberally construed, alleges that  
6 AT&T acted outside the scope of any government certification it  
7 might have received. In particular, paragraphs 81 and 82, which  
8 are incorporated in all of plaintiffs' claims, state:

9 81. On information and belief, the  
10 above-described acts [by defendants] of  
11 interception, disclosure, divulgence and/or use of  
12 Plaintiffs' and class members' communications,  
13 contents of communications, and records pertaining  
14 to their communications occurred without judicial  
15 or other lawful authorization, probable cause,  
16 and/or individualized suspicion.

17 82. On information and belief, at all  
18 relevant times, the government instigated, directed  
19 and/or tacitly approved all of the above-described  
20 acts of AT&T Corp.

21 FAC, ¶¶ 81-82 (emphasis added).

22 Plaintiffs contend that the phrase "occurred without  
23 judicial or other lawful authorization" means that AT&T acted  
24 without a warrant or a certification. Doc #176 (Pl Opp AT&T MTD)  
25 at 13-15. At oral argument, AT&T took issue with this  
26 characterization of "lawful authorization":

27 The emphasis there is on the word 'lawful[.]' When  
28 you read that paragraph in context, it's clear that  
what [plaintiffs are] saying is that any  
authorization [AT&T] receive[s] is, in  
[plaintiffs'] view, unlawful. And you can see that  
because of the other paragraphs in the complaint.  
The very next one, [p]aragraph 82, is the paragraph  
where [plaintiffs] allege that the United States  
government approved and instigated all of our  
actions. It wouldn't be reasonable to construe  
Paragraph 81 as saying that [AT&T was] not  
authorized by the government to do what [AT&T]  
allegedly did when the very next paragraph states  
the exact opposite.

1 6/23/06 Transcript at 10:21-11:6. Indeed, the court does not  
2 question that it would be extraordinary for a large, sophisticated  
3 entity like AT&T to assist the government in a warrantless  
4 surveillance program without receiving a certification to insulate  
5 its actions.

6 Nonetheless, paragraph 81 could be reasonably interpreted  
7 as alleging just that. Even if "the government instigated,  
8 directed and/or tacitly approved" AT&T's alleged actions, it does  
9 not inexorably follow that AT&T received an official certification  
10 blessing its actions. At the hearing, plaintiffs' counsel  
11 suggested that they had "information and belief based on the news  
12 reports that [the alleged activity] was done based on oral  
13 requests" not a written certification. Id at 24:21-22.  
14 Additionally, the phrase "judicial or other lawful authorization"  
15 in paragraph 81 parallels how "a court order" and "a certification"  
16 appear in 18 USC §§ 2511(2)(a)(ii)(A) and (B), respectively; this  
17 suggests that "lawful authorization" refers to a certification.  
18 Interpreted in this manner, plaintiffs are making a factual  
19 allegation that AT&T did not receive a certification.

20 In sum, even if plaintiffs were required to plead  
21 affirmatively that AT&T did not receive a certification authorizing  
22 its alleged actions, plaintiffs' complaint can fairly be  
23 interpreted as alleging just that. Whether and to what extent the  
24 government authorized AT&T's alleged conduct remain issues for  
25 further litigation. For now, however, the court DENIES AT&T's  
26 motion to dismiss on this ground.

27 //

28 //

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

C

AT&T also contends that the complaint should be dismissed because it failed to plead the absence of an absolute common law immunity to which AT&T claims to be entitled. AT&T MTD at 13-15. AT&T asserts that this immunity "grew out of a recognition that telecommunications carriers should not be subject to civil liability for cooperating with government officials conducting surveillance activities. That is true whether or not the surveillance was lawful, so long as the government officials requesting cooperation assured the carrier that it was." Id at 13. AT&T also argues that the statutory immunities do not evince a "congressional purpose to displace, rather than supplement, the common law." Id.

AT&T overstates the case law when intimating that the immunity is long established and unequivocal. AT&T relies primarily on two cases: Halperin v Kissinger, 424 F Supp 838 (DDC 1976), revd on other grounds, 606 F2d 1192 (DC Cir 1979) and Smith v Nixon, 606 F2d 1183 (DC Cir 1979). In Halperin, plaintiffs alleged that the Chesapeake and Potomac Telephone Company (C&P) assisted federal officials in illegally wiretapping plaintiffs' home telephone, thereby violating plaintiffs' constitutional and Title III statutory rights. 424 F Supp at 840. In granting summary judgment for C&P, the district court noted:

//  
//  
//  
//  
//

1 Chesapeake and Potomac Telephone Company, argues  
2 persuasively that it played no part in selecting  
3 any wiretap suspects or in determining the length  
4 of time the surveillance should remain. It  
5 overheard none of plaintiffs' conversations and was  
6 not informed of the nature or outcome of the  
7 investigation. As in the past, C&P acted in  
8 reliance upon a request from the highest Executive  
9 officials and with assurances that the wiretap  
10 involved national security matters. Under these  
11 circumstances, C&P's limited technical role in the  
12 surveillance as well as its reasonable expectation  
13 of legality cannot give rise to liability for any  
14 statutory or constitutional violation.

15 Id at 846.

16 Smith v Nixon involved an allegedly illegal wiretap that  
17 was part of the same surveillance program implicated in Halperin.

18 In addressing C&P's potential liability, the Smith court noted:

19 The District Court dismissed the action against  
20 C&P, which installed the wiretap, on the ground  
21 cited in the District Court's opinion in Halperin:  
22 'C&P's limited technical role in the surveillance  
23 as well as its reasonable expectation of legality  
24 cannot give rise to liability for any statutory or  
25 constitutional violation. \* \* \*.' We think this  
26 was the proper disposition. The telephone company  
27 did not initiate the surveillance, and it was  
28 assured by the highest Executive officials in this  
nation that the action was legal.

606 F2d at 1191 (citation and footnote omitted) (omission in  
original).

The court first observes that Halperin, which formed the  
basis for the Smith decision, never indicated that C&P was "immune"  
from suit; rather, the court granted summary judgment after it  
determined that C&P played only a "limited technical role" in the  
surveillance. And although C&P was dismissed in Smith on a motion  
to dismiss, Smith never stated that C&P was immune from suit; the  
only discussion of "immunity" there related to other defendants who  
claimed entitlement to qualified and absolute immunity.



1 At best, the language in Halperin and Smith is equivocal:  
2 the phrase "C&P's limited technical role in the surveillance as  
3 well as its reasonable expectation of legality cannot give rise to  
4 liability for any statutory or constitutional violation" could  
5 plausibly be interpreted as describing a good faith defense. And  
6 at least one court appears to have interpreted Smith in that  
7 manner. See Manufacturas Intl, Ltda v Manufacturers Hanover Trust  
8 Co, 792 F Supp 180, 192-93 (EDNY 1992) (referring to Smith while  
9 discussing good faith defenses).

10 Moreover, it is not clear at this point in the litigation  
11 whether AT&T played a "mere technical role" in the alleged NSA  
12 surveillance programs. The complaint alleges that "at all relevant  
13 times, the government instigated, directed and/or tacitly approved  
14 all of the above-described acts of AT&T Corp." FAC, ¶ 82. But  
15 given the massive scale of the programs alleged here and AT&T's  
16 longstanding history of assisting the government in classified  
17 matters, one could reasonably infer that AT&T's assistance here is  
18 necessarily more comprehensive than C&P's assistance in Halperin  
19 and Smith. Indeed, there is a world of difference between a single  
20 wiretap and an alleged dragnet that sweeps in the communication  
21 content and records of all or substantially all AT&T customers.

22 AT&T also relies on two Johnson-era cases: Fowler v  
23 Southern Bell Telephone & Telegraph Co, 343 F2d 150 (5th Cir 1965),  
24 and Craska v New York Telephone Co, 239 F Supp 932 (NDNY 1965).  
25 Fowler involved a Georgia state claim for invasion of right of  
26 privacy against a telephone company for assisting federal officers  
27 to intercept plaintiff's telephone conversations. Fowler noted  
28 that a "defense of privilege" would extend to the telephone company

1 only if the court determined that the federal officers acted within  
2 the scope of their duties:

3 If it is established that [the federal officers]  
4 acted in the performance and scope of their  
5 official powers and within the outer perimeter of  
6 their duties as federal officers, then the defense  
7 of privilege would be established as to them. In  
8 this event the privilege may be extended to  
9 exonerate the Telephone Company also if it appears,  
10 in line with the allegations of the complaint, that  
11 the Telephone Company acted for and at the request  
12 of the federal officers and within the bounds of  
13 activity which would be privileged as to the  
14 federal officers.

15 343 F2d at 156-57 (emphasis added). Accordingly, Fowler does not  
16 absolve AT&T of any liability unless and until the court determines  
17 that the government acted legally in creating the NSA surveillance  
18 programs alleged in the complaint.

19 Craska also does not help AT&T. In that case, plaintiff  
20 sued a telephone company for violating her statutory rights by  
21 turning over telephone records to the government under compulsion  
22 of state law. Craska, 239 F Supp at 933-34, 936. The court  
23 declined to ascribe any liability to the telephone company because  
24 its assistance was required under state law: "[T]he conduct of the  
25 telephone company, acting under the compulsion of State law and  
26 process, cannot sensibly be said to have joined in a knowing  
27 venture of interception and divulgence of a telephone conversation,  
28 which it sought by affirmative action to make succeed." Id at 936.  
By contrast, it is not evident whether AT&T was required to help  
the government here; indeed, AT&T appears to have confirmed that it  
did not have any legal obligation to assist the government  
implement any surveillance program. 6/23/06 Transcript at 17:25-  
18:4 ("The Court: Well, AT&T could refuse, could it not, to

1 provide access to its facilities? [AT&T]: Yes, it could. Under  
2 [18 USC §] 2511, your Honor, AT&T would have the discretion to  
3 refuse, and certainly if it believed anything illegal was  
4 occurring, it would do so.").

5           Moreover, even if a common law immunity existed decades  
6 ago, applying it presently would undermine the carefully crafted  
7 scheme of claims and defenses that Congress established in  
8 subsequently enacted statutes. For example, all of the cases cited  
9 by AT&T as applying the common law "immunity" were filed before the  
10 certification provision of FISA went into effect. See § 301 of  
11 FISA. That provision protects a telecommunications provider from  
12 suit if it obtains from the Attorney General or other authorized  
13 government official a written certification "that no warrant or  
14 court order is required by law, that all statutory requirements  
15 have been met, and that the specified assistance is required." 18  
16 USC § 2511(2)(a)(ii)(B). Because the common law "immunity" appears  
17 to overlap considerably with the protections afforded under the  
18 certification provision, the court would in essence be nullifying  
19 the procedural requirements of that statutory provision by applying  
20 the common law "immunity" here. And given the shallow doctrinal  
21 roots of immunity for communications carriers at the time Congress  
22 enacted the statutes in play here, there is simply no reason to  
23 presume that a common law immunity is available simply because  
24 Congress has not expressed a contrary intent. Cf Owen v City of  
25 Independence, 445 US 622, 638 (1980) ("[N]otwithstanding § 1983's  
26 expansive language and the absence of any express incorporation of  
27 common-law immunities, we have, on several occasions, found that a  
28 tradition of immunity was so firmly rooted in the common law and

1 was supported such strong policy reasons that 'Congress would have  
2 specifically so provided had it wished to abolish the doctrine.'" (quoting Pierson v Ray, 386 US 547, 555 (1967)).

3  
4 Accordingly, the court DENIES AT&T's motion to dismiss on  
5 the basis of a purported common law immunity.

6  
7 D

8 AT&T also argues that it is entitled to qualified  
9 immunity. AT&T MTD at 16. Qualified immunity shields state actors  
10 from liability for civil damages "insofar as their conduct does not  
11 violate clearly established statutory or constitutional rights of  
12 which a reasonable person would have known." Harlow v Fitzgerald,  
13 457 US 800, 818 (1982). "Qualified immunity strikes a balance  
14 between compensating those who have been injured by official  
15 conduct and protecting government's ability to perform its  
16 traditional functions." Wyatt v Cole, 504 US 158, 167 (1992).  
17 "[T]he qualified immunity recognized in Harlow acts to safeguard  
18 government, and thereby to protect the public at large, not to  
19 benefit its agents." Wyatt v Cole, 504 US 158, 168 (1992).  
20 Compare AT&T MTD at 17 ("It would make little sense to protect the  
21 principal but not its agent."). The Supreme Court does not "draw a  
22 distinction for purposes of immunity law between suits brought  
23 against state officials under [42 USC] § 1983 and suits brought  
24 directly under the Constitution [via Bivens v Six Unknown Named  
25 Agents, 403 US 388 (1971)] against federal officials." Butz v  
26 Economou, 438 US 478, 504 (1978).

27 //

28 //

1 At the pleadings stage, qualified immunity analysis  
2 entails three steps. First, the court must determine whether,  
3 taken in the light most favorable to the plaintiff, the facts  
4 alleged show a violation of the plaintiffs' statutory or  
5 constitutional rights. Saucier v Katz, 533 US 194, 201 (2001). If  
6 a violation has been alleged, the court next determines whether the  
7 right infringed was clearly established at the time of the alleged  
8 violation. Finally, the court assesses whether it would be clear  
9 to a reasonable person in the defendant's position that its conduct  
10 was unlawful in the situation it confronted. *Id.* at 202, 205. See  
11 also Frederick v Morse, 439 F3d 1114, 1123 (9th Cir 2006)  
12 (characterizing this final inquiry as a discrete third step in the  
13 analysis). "This is not to say that an official action is  
14 protected by qualified immunity unless the very action in question  
15 has previously been held unlawful, but it is to say that in the  
16 light of pre-existing law the unlawfulness must be apparent." Hope  
17 v Pelzer, 536 US 730, 739 (2002) (citation omitted).

18  
19 1

20 When a private party seeks to invoke qualified immunity,  
21 the court must first decide whether qualified immunity is  
22 "categorically available," which "requires an evaluation of the  
23 appropriateness of qualified immunity given its historical  
24 availability and the policy considerations underpinning the  
25 doctrine." Jensen v Lane County, 222 F3d 570, 576 (9th Cir 2000).  
26 This inquiry is distinct from the question whether a nominally  
27 private party is a state actor for purposes of a section 1983 or  
28 Bivens claim.

1 In Wyatt v Cole, 504 US 158 (1992), the Supreme Court  
2 laid the foundation for determining whether a private actor is  
3 entitled to qualified immunity. The plaintiff there sued under  
4 section 1983 to recover property from a private party who had  
5 earlier obtained a writ of replevin against the plaintiff. See  
6 Lugar v Edmondson Oil Co, 457 US 922 (1982) (holding that a private  
7 party acted under color of law under similar circumstances). After  
8 determining that the common law did not recognize an immunity from  
9 analogous tort suits, the court "conclude[d] that the rationales  
10 mandating qualified immunity for public officials are not  
11 applicable to private parties." Wyatt, 504 US at 167. Although  
12 Wyatt purported to be limited to its facts, *id* at 168, the broad  
13 brush with which the Court painted suggested that private parties  
14 could rarely, if ever, don the cloak of qualified immunity. See  
15 also Ace Beverage Co v Lockheed Information Mgmt Servs, 144 F3d  
16 1218, 1219 n3 (9th Cir 1998) (noting that "[i]n cases decided  
17 before [the Supreme Court's decision in Richardson v McKnight, 521  
18 US 399 (1997)]," the Ninth Circuit had "adopted a general rule that  
19 private parties are not entitled to qualified immunity").

20 Applying Wyatt to a case involving section 1983 claims  
21 against privately employed prison guards, the Supreme Court in  
22 Richardson v McKnight, 521 US 399 (1997), stated that courts should  
23 "look both to history and to the purposes that underlie government  
24 employee immunity in order to" determine whether that immunity  
25 extends to private parties. *Id* at 404. Although this issue has  
26 been addressed by the Ninth Circuit in several cases, the court has  
27 yet to extend qualified immunity to a private party under McKnight.  
28 See, e g, Ace Beverage, 144 F3d at 1220; Jensen, 222 F3d at 576-80.

1  
2 The court now determines whether the history of the  
3 alleged immunity and purposes of the qualified immunity doctrine  
4 support extending qualified immunity to AT&T.

5 As described in section II(C), *supra*, no firmly rooted  
6 common law immunity exists for telecommunications providers  
7 assisting the government. And presently applying whatever immunity  
8 might have previously existed would undermine the various statutory  
9 schemes created by Congress, including the certification defense  
10 under 18 USC § 2511(2)(a)(ii)(B).

11 Turning to the purposes of qualified immunity, they  
12 include: "(1) protecting the public from unwarranted timidity on  
13 the part of public officials and encouraging the vigorous exercise  
14 of official authority; (2) preventing lawsuits from distracting  
15 officials from their governmental duties; and (3) ensuring that  
16 talented candidates are not deterred by the threat of damages suits  
17 from entering public service." Jensen, 222 F3d at 577 (citations,  
18 quotations and alterations omitted). See also Harlow, 457 US at  
19 816 (recognizing "the general costs of subjecting officials to the  
20 risks of trial -- distraction of officials from their governmental  
21 duties, inhibition of discretionary action, and deterrence of able  
22 people from public service"). AT&T contends that national security  
23 surveillance is "a traditional governmental function of the highest  
24 importance" requiring access to the "critical telecommunications  
25 infrastructure" that companies such as AT&T would be reluctant to  
26 furnish if they were exposed to civil liability. AT&T MTD at 17.

27 //

28 //

1 AT&T's concerns, while relevant, do not warrant extending  
2 qualified immunity here because the purposes of that immunity are  
3 already well served by the certification provision of 18 USC §  
4 2511(2)(a)(ii). As noted above, although it is unclear whether a  
5 valid certification would bar plaintiffs' constitutional claim,  
6 section 2511(2)(a)(ii) clearly states that a valid certification  
7 precludes the statutory claims asserted here. See *supra* I(G)(1).  
8 Hence, but for the government's assertion of the state secrets  
9 privilege, the certification provision would seem to facilitate  
10 prompt adjudication of damages claims such as those at bar. And  
11 because section 2511(2)(a)(ii)'s protection does not appear to  
12 depend on a fact-intensive showing of good faith, the provision  
13 could be successfully invoked without the burdens of full-blown  
14 litigation. Compare Tapley v Collins, 211 F3d 1210, 1215 (11th Cir  
15 2000) (discussing the differences between qualified immunity and  
16 good faith defense under Title III, 18 USC § 2520(d)).

17 More fundamentally, "[w]hen Congress itself provides for  
18 a defense to its own cause of action, it is hardly open to the  
19 federal court to graft common law defenses on top of those Congress  
20 creates." Berry v Funk, 146 F3d 1003, 1013 (DC Cir 1998) (holding  
21 that qualified immunity could not be asserted against a claim under  
22 Title III). As plaintiffs suggest, the Ninth Circuit appears to  
23 have concluded that the only defense under Title III is that  
24 provided for by statute -- although, in fairness, the court did not  
25 explicitly address the availability of qualified immunity. See  
26 Jacobson v Rose, 592 F2d 515, 522-24 (9th Cir 1978) (joined by  
27 then-Judge Kennedy). But cf Doe v United States, 941 F2d 780, 797-  
28 99 (9th Cir 1991) (affirming grant of qualified immunity from



1 liability under section 504 of the Rehabilitation Act without  
2 analyzing whether qualified immunity could be asserted in the first  
3 place). Nonetheless, at least two appellate courts have concluded  
4 that statutory defenses available under Title III do not preclude a  
5 defendant from asserting qualified immunity. Blake v Wright, 179  
6 F3d 1003, 1013 (6th Cir 1999) (The court "fail[ed] to see the logic  
7 of providing a defense of qualified immunity to protect public  
8 officials from personal liability when they violate constitutional  
9 rights that are not clearly established and deny them qualified  
10 immunity when they violate statutory rights that similarly are not  
11 clearly established."); accord Tapley, 211 F3d at 1216. But see  
12 Mitchell v Forsyth, 472 US 511, 557 (1985) (Brennan concurring in  
13 part and dissenting in part) ("The Court's argument seems to be  
14 that the trial court should have decided the legality of the  
15 wiretap under Title III before going on to the qualified immunity  
16 question, since that question arises only when considering the  
17 legality of the wiretap under the Constitution.").

18 With all due respect to the Sixth and Eleventh Circuits,  
19 those courts appear to have overlooked the relationship between the  
20 doctrine of qualified immunity and the schemes of state and federal  
21 official liability that are essentially creatures of the Supreme  
22 Court. Qualified immunity is a doctrinal outgrowth of expanded  
23 state actor liability under 42 USC § 1983 and Bivens. See Monroe v  
24 Pape, 365 US 167 (1961) (breathing new life into section 1983);  
25 Scheuer v Rhodes, 416 US 232, 247 (1974) (deploying the phrase  
26 "qualified immunity" for the first time in the Supreme Court's  
27 jurisprudence); Butz v Economou, 438 US 478 (1978) (extending  
28 qualified immunity to federal officers sued under Bivens for

1 federal constitutional violations); Maine v Thiboutot, 448 US 1  
2 (1980) (holding that section 1983 could be used to vindicate non-  
3 constitutional statutory rights); Harlow, 457 US at 818 (making the  
4 unprecedented reference to "clearly established statutory" rights  
5 just two years after Thiboutot (emphasis added)). These causes of  
6 action "were devised by the Supreme Court without any legislative  
7 or constitutional (in the sense of positive law) guidance."  
8 Crawford-El v Britton, 93 F3d 813, 832 (DC Cir 1996) (en banc)  
9 (Silberman concurring), vacated on other grounds, 523 US 574  
10 (1998). "It is understandable then, that the Court also developed  
11 the doctrine of qualified immunity to reduce the burden on public  
12 officials." Berry, 146 F3d at 1013.

13 In contrast, the statutes in this case set forth  
14 comprehensive, free-standing liability schemes, complete with  
15 statutory defenses, many of which specifically contemplate  
16 liability on the part of telecommunications providers such as AT&T.  
17 For example, the Stored Communications Act prohibits providers of  
18 "electronic communication service" and "remote computing service"  
19 from divulging contents of stored communications. See 18 USC §  
20 2702(a)(1), (a)(2). Moreover, the Stored Communications Act  
21 specifically contemplates carrier liability for unauthorized  
22 disclosure of subscriber records "to any governmental entity." See  
23 id § 2702(a)(3). It can hardly be said that Congress did not  
24 contemplate that carriers might be liable for cooperating with the  
25 government when such cooperation did not conform to the  
26 requirements of the act.

27 //

28 //

1 Similarly, Congress specifically contemplated that  
2 communications carriers could be liable for violations of Title  
3 III. See Jacobson, 592 F2d at 522. And in providing for a "good  
4 faith" defense in Title III, Congress specifically sought "to  
5 protect telephone companies or other persons who cooperate \* \* \*  
6 with law enforcement officials.'" Id at 522-23 (quoting Senate  
7 debates). See also id at 523 n 13. Cf 18 USC § 2511(2)(a)(ii)  
8 (providing a statutory defense to "providers of wire or electronic  
9 communication service").

10 In sum, neither the history of judicially created  
11 immunities for telecommunications carriers nor the purposes of  
12 qualified immunity justify allowing AT&T to claim the benefit of  
13 the doctrine in this case.

14  
15 3

16 The court also notes that based on the facts as alleged  
17 in plaintiffs' complaint, AT&T is not entitled to qualified  
18 immunity with respect to plaintiffs' constitutional claim, at least  
19 not at this stage of the proceedings. Plaintiffs' constitutional  
20 claim alleges that AT&T provides the government with direct and  
21 indiscriminate access to the domestic communications of AT&T  
22 customers. See, e g, FAC, ¶ 42 ("On information and belief, AT&T  
23 Corp has provided and continues to provide the government with  
24 direct access to all or a substantial number of the communications  
25 transmitted through its key domestic telecommunications facilities,  
26 including direct access to streams of domestic, international and  
27 foreign telephone and Internet communications."); id, ¶ 78  
28 (incorporating paragraph 42 by reference into plaintiffs'

1 constitutional claim). In United States v United States District  
2 Court, 407 US 297 (1972) (Keith), the Supreme Court held that the  
3 Fourth Amendment does not permit warrantless wiretaps to track  
4 domestic threats to national security, id at 321, reaffirmed the  
5 "necessity of obtaining a warrant in the surveillance of crimes  
6 unrelated to the national security interest," id at 308, and did  
7 not pass judgment "on the scope of the President's surveillance  
8 power with respect to the activities of foreign powers, within or  
9 without this country," id. Because the alleged dragnet here  
10 encompasses the communications of "all or substantially all of the  
11 communications transmitted through [AT&T's] key domestic  
12 telecommunications facilities," it cannot reasonably be said that  
13 the program as alleged is limited to tracking foreign powers.  
14 Accordingly, AT&T's alleged actions here violate the constitutional  
15 rights clearly established in Keith. Moreover, because "the very  
16 action in question has previously been held unlawful," AT&T cannot  
17 seriously contend that a reasonable entity in its position could  
18 have believed that the alleged domestic dragnet was legal.

19  
20  
21  
22  
23  
24  
25  
26  
27  
28

4

Accordingly, the court DENIES AT&T's instant motion to  
dismiss on the basis of qualified immunity. The court does not  
preclude AT&T from raising the qualified immunity defense later in  
these proceedings, if further discovery indicates that such a  
defense is merited.

//  
//  
//

## III

1  
2 As this case proceeds to discovery, the court flags a few  
3 procedural matters on which it seeks the parties' guidance. First,  
4 while the court has a duty to the extent possible to disentangle  
5 sensitive information from nonsensitive information, see Ellsberg,  
6 709 F2d at 57, the court also must take special care to honor the  
7 extraordinary security concerns raised by the government here. To  
8 help perform these duties, the court proposes appointing an expert  
9 pursuant to FRE 706 to assist the court in determining whether  
10 disclosing particular evidence would create a "reasonable danger"  
11 of harming national security. See FRE 706(a) ("The court may on  
12 its own motion or on the motion of any party enter an order to show  
13 cause why expert witnesses should not be appointed, and may request  
14 the parties to submit nominations. The court may appoint any  
15 expert witnesses agreed upon by the parties, and may appoint expert  
16 witnesses of its own selection."). Although other courts do not  
17 appear to have used FRE 706 experts in the manner proposed here,  
18 this procedural innovation seems appropriate given the complex and  
19 weighty issues the court will confront in navigating any future  
20 privilege assertions. See Ellsberg, 709 F2d at 64 (encouraging  
21 "procedural innovation" in addressing state secrets issues);  
22 Halpern, 258 F2d at 44 ("A trial *in camera* in which the privilege  
23 relating to state secrets may not be availed of by the United  
24 States is permissible, if, in the judgment of the district court,  
25 such a trial can be carried out without substantial risk that  
26 secret information will be publicly divulged").

27 //

28 //

1           The court contemplates that the individual would be one  
2 who had a security clearance for receipt of the most highly  
3 sensitive information and had extensive experience in intelligence  
4 matters. This individual could perform a number of functions;  
5 among others, these might include advising the court on the risks  
6 associated with disclosure of certain information, the manner and  
7 extent of appropriate disclosures and the parties' respective  
8 contentions. While the court has at least one such individual in  
9 mind, it has taken no steps to contact or communicate with the  
10 individual to determine availability or other matters. This is an  
11 appropriate subject for discussion with the parties.

12           The court also notes that should it become necessary for  
13 the court to review additional classified material, it may be  
14 preferable for the court to travel to the location of those  
15 materials than for them to be hand-carried to San Francisco. Of  
16 course, a secure facility is available in San Francisco and was  
17 used to house classified documents for a few days while the court  
18 conducted its *in camera* review for purposes of the government's  
19 instant motion. The same procedures that were previously used  
20 could be employed again. But alternative procedures may also be  
21 used and may in some instances be more appropriate.

22           Finally, given that the state secrets issues resolved  
23 herein represent controlling questions of law as to which there is  
24 a substantial ground for difference of opinion and that an  
25 immediate appeal may materially advance ultimate termination of the  
26 litigation, the court certifies this order for the parties to apply  
27 for an immediate appeal pursuant to 28 USC § 1292(b). The court  
28 notes that if such an appeal is taken, the present proceedings do

1 not necessarily have to be stayed. 28 USC § 1292(b)  
2 (“[A]pplication for an appeal hereunder shall not stay proceedings  
3 in the district court unless the district judge or the Court of  
4 Appeals or a judge thereof shall so order.”). At the very least,  
5 it would seem prudent for the court to select the expert pursuant  
6 to FRE 706 prior to the Ninth Circuit’s review of this matter.

7           Accordingly, the court ORDERS the parties to SHOW CAUSE  
8 in writing by July 31, 2006, why it should not appoint an expert  
9 pursuant to FRE 706 to assist in the manner stated above. The  
10 responses should propose nominees for the expert position and  
11 should also state the parties’ views regarding the means by which  
12 the court should review any future classified submissions.  
13 Moreover, the parties should describe what portions of this case,  
14 if any, should be stayed if this order is appealed.

15 //  
16 //  
17 //  
18 //  
19 //  
20 //  
21 //  
22 //  
23 //  
24 //  
25 //  
26 //  
27 //  
28 //

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

IV

In sum, the court DENIES the government's motion to dismiss, or in the alternative, for summary judgment on the basis of state secrets and DENIES AT&T's motion to dismiss. As noted in section III, *supra*, the parties are ORDERED TO SHOW CAUSE in writing by July 31, 2006, why the court should not appoint an expert pursuant to FRE 706 to assist the court. The parties' briefs should also address whether this action should be stayed pending an appeal pursuant to 28 USC § 1292(b).

The parties are also instructed to appear on August 8, 2006, at 2 PM, for a further case management conference.

IT IS SO ORDERED.



---

VAUGHN R WALKER  
United States District Chief Judge