IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, et al,

Plaintiffs,

v

AT&T CORPORATION, et al,

Defendants.

/

No C-06-672 VRW

ORDER

Plaintiffs allege that AT&T Corporation (AT&T) and its holding company, AT&T Inc, are collaborating with the National Security Agency (NSA) in a massive warrantless surveillance program that illegally tracks the domestic and foreign communications and communication records of millions of Americans. The first amended complaint (Doc #8 (FAC)), filed on February 22, 2006, claims that AT&T and AT&T Inc have committed violations of:

(1) The First and Fourth Amendments to the United States Constitution (acting as agents or instruments of the government) by illegally intercepting, disclosing, divulging and/or using plaintiffs' communications;

(2) Section 109 of Title I of the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 USC § 1809, by engaging in illegal electronic surveillance of plaintiffs' communications under color of law;

(3) Section 802 of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by section 101 of Title I of the Electronic Communications Privacy Act of 1986 (ECPA), 18 USC §§ 2511(1)(a), (1)(c), (1)(d) and (3)(a), by illegally intercepting, disclosing, using and/or divulging plaintiffs' communications;

(4) Section 705 of Title VII of the Communications Act of 1934, as amended, 47 USC § 605, by unauthorized divulgence and/or publication of plaintiffs' communications;

(5) Section 201 of Title II of the ECPA ("Stored Communications Act"), as amended, 18 USC §§ 2702(a)(1) and (a)(2), by illegally divulging the contents of plaintiffs' communications;

(6) Section 201 of the Stored Communications Act, as amended by section 212 of Title II of the USA PATRIOT Act, 18 USC § 2702(a)(3), by illegally divulging records concerning plaintiffs' communications to a governmental entity and

(7) California's Unfair Competition Law, Cal Bus & Prof Code §§ 17200 et seq, by engaging in unfair, unlawful and deceptive business practices.

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

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

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

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

At a May 17, 2006, hearing, the court requested additional briefing from the parties addressing (1) whether this case could be decided without resolving the state secrets issue, thereby obviating any need for the court to review the government's classified submissions and (2) whether the state secrets issue is implicated by an FRCP 30(b)(6) deposition request for information about any certification that AT&T may have received from the government authorizing the alleged wiretapping activities. Based on the parties' submissions, the court concluded in a June 6, 2006, order that this case could not proceed and discovery could not commence until the court examined *in camera* and *ex parte* the classified documents to assess whether and to what extent the state secrets privilege applies. Doc #171.

After performing this review, the court heard oral argument on the motions to dismiss on June 23, 2006. For the reasons discussed herein, the court DENIES the government's motion to dismiss and DENIES AT&T's motion to dismiss.

I

The court first addresses the government's motion to dismiss or, alternatively, for judgment on state secrets grounds. After exploring the history and principles underlying the state secrets privilege and summarizing the government's arguments, the court turns to whether the state secrets privilege applies and requires dismissal of this action or immediate entry of judgment in favor of defendants. The court then takes up how the asserted privilege bears on plaintiffs' discovery request for any government certification that AT&T might have received authorizing the alleged

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

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.

//

//

//

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

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

Id at 106, quoted in Tenet v Doe, 544 US 1, 7-8 (2005). Hence, given the secrecy implied in such a contract, the Totten Court "thought it entirely incompatible with the nature of such a 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.**

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

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

//

//

//

//

> 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B

Relying on Kasza, the government advances three reasons why the state secrets privilege requires dismissing this action or granting summary judgment for AT&T: (1) the very subject matter of 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.

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

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

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

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

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

//

//

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

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

C

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

//

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.

//

//

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

Id.

Attorney General Alberto Gonzales subsequently confirmed that this program intercepts "contents of communications where * * * one party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." Doc #87 (AT&T Request for Judicial Notice), Ex J at 1 (hereinafter "12/19/05 Press Briefing"), available at http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html (last visited July 19, 2005). The Attorney General also noted, "This [program] is not about wiretapping everyone. This is a very concentrated, very limited program focused at gaining information about our enemy." Id at 5. The President has also made a public statement, of which the court takes judicial notice, that the government's "international activities strictly target al Qaeda and their known affiliates," "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.

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

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

> In the Fall of 2001 * * * while Mr Nacchio was Chairman and CEO of Qwest and was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee, Qwest was approached to permit the Government access to the private telephone records of Qwest customers.
>
> Mr Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted and that there was a disinclination on the part of the authorities to use any legal process, including the Special Court which had been established to handle such matters, Mr Nacchio concluded that these requests violated the privacy requirements of the Telecommications [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.

Markman Decl, Ex 6.

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

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

News Release, BellSouth Statement on Governmental Data Collection (May 15, 2006), available at http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860 (last visited July 19, 2006). Although declining to confirm or deny whether it had any relationship to the NSA program acknowledged by the President, Verizon stated in relevant part:

> One of the most glaring and repeated falsehoods in the media reporting is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls.
>
> This is false. From the time of the 9/11 attacks until just four months ago, Verizon had three major businesses - its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of these businesses, or any call data from those records. None of these companies –– wireless or wireline –– provided customer records or call data.

See News Release, Verizon Issues Statement on NSA Media Coverage (May 16, 2006), available at 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

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

2

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

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

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

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

D

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

//

//

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

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

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

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

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

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

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

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

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

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

E

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

1

Although the principles announced in Totten, Tenet, Reynolds and Kasza inform the court's decision here, those cases are not strictly analogous to the facts at bar.

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

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

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

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

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

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

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

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

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

//

//

//

The court's conclusion here follows the path set in Halkin v Helms and Ellsberg v Mitchell, the two cases most factually similar to the present. The Halkin and Ellsberg courts did not preclude suit because of a Totten-based implied covenant of silence. Although the courts eventually terminated some or all of plaintiffs' claims because the privilege barred discovery of certain evidence (Halkin I, 598 F2d at 10; Halkin II, 690 F2d at 980, 987-88; Ellsberg, 709 F2d at 65), the courts did not dismiss the cases at the outset, as would have been required had the Totten bar applied. Accordingly, the court sees no reason to apply the Totten bar here.

For all of the above reasons, the court declines to dismiss this case based on the categorical Totten/Tenet bar.

2

The court must also dismiss this case if "the very subject matter of the action" is a state secret and therefore "any further proceeding * * * would jeopardize national security." Kasza, 133 F3d at 1170. As a preliminary matter, the court agrees that the government has satisfied the three threshold requirements for properly asserting the state secrets privilege: (1) the head of the relevant department, Director of National Intelligence John D Negroponte (2) has lodged a formal claim of privilege (Negroponte Decl, ¶¶ 9, 13) (3) after personally considering the matter (Id, ¶¶ 2, 9, 13). Moreover, the Director of the NSA, Lieutenant General Keith B Alexander, has filed a declaration supporting Director Negroponte's assertion of the privilege. Alexander Decl, ¶¶ 2, 9.

//

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

//

//

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

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

3

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

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

4

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

F

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

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

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

//

//

//

//

//

//

//

//

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.").

//

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

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

3

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

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

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

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

4

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

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

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

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

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

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

5

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

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

H

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

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

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

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

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

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

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

//

//

//

//

//

//

//

//

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.

//

//

//

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

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

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

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

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

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

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

//

//

//

//

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

> **Whether styled as a constitutional or prudential limit on standing, the Court has sometimes determined that where large numbers of Americans suffer alike, the political process, rather than the judicial process, may provide the more appropriate remedy for a widely shared grievance.**
>
> **[This] kind of judicial language * * * however, invariably appears in cases where the harm at issue is not only widely shared, but is also of an abstract and indefinite nature.**

Id at 23. The Court continued:

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

Id at 24.

Here, the alleged injury is concrete even though it is widely shared. Despite AT&T's alleged creation of a dragnet to intercept all or substantially all of its customers' 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.

//

//

//

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

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

//

//

//

//

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.**

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

> **A civil action will not lie [under 18 USC § 2520] where the requirements of sections 2511(2)(a)(ii) of title 18 are met. With regard to that exception, the Committee intends that the following procedural standards will apply:**
>
> > **(1) The complaint must allege that a wire or electronic communications service provider (or one of its employees) (a) disclosed the existence of a wiretap; (b) acted without a facially valid court order or certification; (c) acted beyond the scope of a court order or certification or (d) acted on bad faith. Acting in bad faith would include failing to read the order or collusion. If the complaint fails to make any of these allegations, the defendant can move to dismiss the complaint for failure to state a claim upon which relief can be granted.**

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

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

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

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

> 81. On information and belief, the above-described acts [by defendants] of interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications occurred without judicial or other lawful authorization, probable cause, and/or individualized suspicion.
>
> 82. On information and belief, at all relevant times, the government instigated, directed and/or tacitly approved all of the above-described acts of AT&T Corp.

FAC, ¶¶ 81-82 (emphasis added).

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

> The emphasis there is on the word 'lawful[.'] When 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.

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

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

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

//

//

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:

//

//

//

//

//

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

Id at 846.

Smith v Nixon involved an allegedly illegal wiretap that was part of the same surveillance program implicated in Halperin. In addressing C&P's potential liability, the Smith court noted:

> The District Court dismissed the action against C&P, which installed the wiretap, on the ground cited in the District Court's opinion in Halperin: 'C&P's limited technical role in the surveillance as well as its reasonable expectation of legality cannot give rise to liability for any statutory or constitutional violation. * * *.' We think this was the proper disposition. The telephone company did not initiate the surveillance, and it was 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.

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

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

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

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

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

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

Craska also does not help AT&T. In that case, plaintiff sued a telephone company for violating her statutory rights by turning over telephone records to the government under compulsion of state law. Craska, 239 F Supp at 933-34, 936. The court declined to ascribe any liability to the telephone company because its assistance was required under state law: "[T]he conduct of the telephone company, acting under the compulsion of State law and process, cannot sensibly be said to have joined in a knowing venture of interception and divulgence of a telephone conversation, 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

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

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

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

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

D

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

//

//

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

1

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

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

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

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

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

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

//

//

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

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

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

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

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

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

//

//

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

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

3

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

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

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

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

//

//

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

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

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

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

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

//

//

//

//

//

//

//

//

//

//

//

//

//

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