IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

STUDS TERKEL, et al.,	)	
	)	
Plaintiffs,	)	
	)	
vs.	)	**Case No. 06 C 2837**
	)	
AT&T CORP., et al.,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

MATTHEW F. KENNELLY, District Judge:

This case is one of a number of suits filed in federal courts around the country in which the plaintiffs contend that AT&T Corp. and affiliated entities have illegally provided information about customer telephone calls and Internet communications to the National Security Agency. Some of the cases have been stayed; a few, including this one, have not. The government has intervened in the cases that are being litigated and has sought dismissal pursuant to the "state secrets" privilege, contending that allowing the cases to be litigated would damage national security. In the one case that has reached decision thus far, *Hepting v. AT&T Corp.,* Case No. C-06-672 (N.D. Cal. July 21, 2006), the Honorable Vaughn Walker concluded that the state secrets privilege did not require dismissal of the case, largely because of public disclosures by the government about a program in which it intercepts the contents of communications in certain circumstances and public admissions by AT&T about its willingness to assist the government.

This case differs from *Hepting* in two significant respects. First, the plaintiffs in this case do not challenge the interception of the *contents* of communications; their challenge is limited to the alleged disclosure of *records* regarding customer communications. The governmental disclosures that Judge Walker relied on in *Hepting* concern the former, not the latter. Second, the plaintiffs in this case seek (thus far, at least) only prospective relief – an injunction and a declaratory judgment – in contrast to the *Hepting* plaintiffs, who also seek damages for claimed past disclosures. In view of constitutionally-imposed limits on the standing of a plaintiff to sue for prospective relief, disclosures about past activities (of the type relied upon by Judge Walker in *Hepting*) are of limited value to the plaintiffs in the present case, as we will discuss.[1]

The plaintiffs in this case, six individuals and the American Civil Liberties Union of Illinois, seek to represent a class consisting of all of AT&T's Illinois customers. They allege that AT&T has released and continues to release records regarding "massive numbers of domestic telephone calls" involving its Illinois customers to the NSA, in violation of 18 U.S.C. § 2702(a)(3), and that the NSA uses this data to search for patterns that might warrant further investigation. *See* Amend. Compl. ¶ 2.

---

1 The Court has two other similar cases pending. In one of them, *Joll v. AT&T Corp.,* Case No. 06 C 2680 (N.D. Ill.), the plaintiffs, as in *Hepting,* challenge the alleged interception of contents of communications as well as the alleged disclosure of records, and they seek damages for past alleged wrongs as well as prospective relief. *See, e.g.,* Second Am. Compl. (Case No. 06 C 2680, docket no. 31) ¶¶ 2, 35, 57-62. In the other case, *Waxman v. AT&T Corp.,* Case No. 06 C 2900 (N.D. Ill.), the plaintiffs challenge only the alleged disclosure of records, but they seek damages for past alleged violations in addition to injunctive relief. *See, e.g.,* Compl. (Case No. 06 C 2900, docket no. 1) ¶¶ 1, 9-11, 18, 25, 27, 31, 37. The Court temporarily deferred consideration of those cases in order to focus on the present case, in which the plaintiffs had moved for entry of a preliminary injunction. Because of the differences between those cases and this one, our ruling in this case is not necessarily dispositive of the other cases.

AT&T has moved to dismiss the complaint, contending that the plaintiffs have inadequately alleged their standing to sue. The government, to which the Court granted leave to intervene, has moved to dismiss or for summary judgment, arguing that the state secrets privilege and various other legal doctrines bar the litigation of the case in its entirety, or at a minimum prevent the plaintiffs from seeking to establish their standing to sue.

For the reasons stated below, the Court denies AT&T's motion to dismiss, concluding that the complaint adequately alleges the plaintiffs' standing. We grant, however, the government's motion to dismiss. The Court concludes that in contrast to the alleged content monitoring that is a key focus of the *Hepting* case, there have been no public disclosures of the existence or non-existence of AT&T's claimed record turnover – the sole focus of the current complaint in the present case – that are sufficient to overcome the government's assertion of the state secrets privilege. The Court further concludes that due to the operation of that privilege, the plaintiffs (to whom we will refer as the "*Terkel* plaintiffs") cannot obtain the information they would need to prove their standing to sue for prospective relief and thus cannot maintain that type of claim. We therefore dismiss the *Terkel* plaintiffs' complaint, allowing them to seek leave to amend their claims if they wish to do so.

Facts

As noted above, the *Terkel* plaintiffs are six Illinois residents and an organization, the ACLU of Illinois. They have filed this action seeking to represent all present and future Illinois residents who are or will become AT&T customers. The ACLU of Illinois, an organization dedicated to the protection of civil liberties and civil rights, seeks to serve as the representative of its members who are Illinois residents and AT&T customers. Am. Compl. ¶¶ 3-4, 14, 16.

AT&T Corp. is the largest telecommunications company in the United States. Directly and through its affiliates and subsidiaries, including Illinois Bell Telephone Co., AT&T provides telephone and Internet services to millions of customers across the country. *Id.* ¶ 15.

The *Terkel* plaintiffs allege that in the aftermath of the September 11, 2001 terrorist attacks, AT&T began providing to the National Security agency records concerning the telephone calls of its customers. These records, the plaintiffs claim, include the originating and receiving telephone numbers for calls, as well as the date, time and duration of calls. Plaintiffs allege that AT&T has provided and continues to provide these records to the NSA without legal authorization or adequate justification. Based on these allegations, the plaintiffs seek a declaratory judgment that AT&T's actions violate the Electronic Communications Privacy Act, 18 U.S.C. § 2702(a)(3), and an injunction barring such violations in the future. Am. Compl. ¶¶ 21-25 & Part VII.

Together with their amended complaint, the *Terkel* plaintiffs filed a motion for a preliminary injunction, a motion for class certification, and a motion for leave to take expedited discovery in anticipation of a hearing on their preliminary injunction motion. Specifically, the *Terkel* plaintiffs sought permission to serve AT&T with a set of interrogatories in which they requested (in summary) the following information: whether AT&T has provided or continues to provide customer telephone records to the government, either pursuant to specific laws or without statutory authorization; identification of any governmental entities to which AT&T has provided or will provide such records; and how many AT&T customers' records have been disclosed. *See generally*, Pl. Mot. to Permit Ltd. Disc., Ex. 1.

The government sought leave to intervene in the case, arguing that the plaintiffs' allegations implicated matters vital to national security. The Court granted the government's motion. Both AT&T and the government filed motions to dismiss; the government's motion also includes a request for summary judgment. The Court deferred consideration of the *Terkel* plaintiffs' preliminary injunction and class certification motions pending determination of the motions to dismiss.

AT&T's motion to dismiss, as noted earlier, concerned the alleged inadequacy of the allegations in the plaintiffs' complaint. The government's motion included publicly-filed affidavits from Director of National Intelligence John Negroponte and National Security Agency Director and Lieutenant General Keith Alexander, setting forth facts supporting the government's contention that the state secrets privilege and other legal doctrines required dismissal of the case. In its motion, the government also gave notice that it was filing for the Court's *ex parte, in camera* review additional declarations by Mr. Negroponte and Lt. Gen. Alexander containing classified material. The Court thoroughly reviewed the classified materials in chambers under carefully controlled security.[2] This publicly-issued decision is not premised in any way, shape, or form on the classified materials or their contents. We are issuing

---

2 Only one copy of the materials was provided, and following our review, the materials were removed to a secure location outside the Court's control (we reviewed the materials again on later occasions under similar conditions). The Court was not permitted to discuss the materials with other members of our staff, and notes that we took were removed and kept in a secure location outside the Court's control. We advised the parties that we needed to ask the government's counsel questions about the material; this was done in an *in camera, ex parte* session on July 13, 2006 that was tape recorded so that a transcript could later be made by personnel with appropriate security clearance (we have reviewed the transcript of the July 13 session and believe it to be accurate). The Court asked the government to provide further information about certain matters in the classified materials; this information was thereafter produced for *in camera*, *ex parte* inspection as well.

on this date a separate Memorandum discussing various points arising from the classified materials; because that Memorandum discusses certain of the contents of those materials, it, too, is classified and will be unavailable for inspection by the public or any of the parties or counsel in this case other than counsel for the government. The Court directs counsel for the government to cause the classified Memorandum be placed in a secure location and to ensure its availability in the event of appellate review.

Discussion

A. Plaintiff's claim under 18 U.S.C. § 2702(a)(3)

Under section 2702(a)(3),

> a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

The *Terkel* plaintiffs contend that AT&T has violated this statute by providing large quantities of customer telephone records to the federal government without legal authorization or adequate justification. Specifically, plaintiffs allege that AT&T knowingly and intentionally provides the federal government with telephone records that document the telephone numbers from which calls are made, the telephone numbers at which the calls are received, and the dates and times at which the calls begin and end. Amend. Compl. ¶¶ 21-22. Plaintiffs allege that AT&T disclosed their records without statutory authorization, without prior consent from its customers, and without any other legal justification. *Id.* ¶¶ 23-25.

This provision of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 *et seq.*, was added as part of the USA PATRIOT Act of 2001, Pub. L. No. 107-86, 115 Stat. 272 (2001), reauthorized by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub.

L. No. 109-177, 120 Stat. 192 (2005). Unfortunately, there is no legislative history regarding the adoption of this specific provision of the ECPA. There is, however, a House Judiciary Committee report regarding the initial version of the ECPA which provides insight into the purposes behind regulating telecommunications companies' ability to share customer records with third parties. H.R. REP. NO. 99-647, at 64-73 (1986).

The original version of the ECPA dealt primarily with the disclosure of the contents of electronic communications, rather than records of communications. In its report, the House Judiciary Committee commented on the need to protect privacy interests to ensure that advances in technology do not lead to erosions of personal privacy. *Id.* at 19. The Committee stated that

> subscribers and customers of remote computing services should be afforded a level of confidence that the contents of records maintained on their behalf for the purpose of providing remote computing services will not be disclosed or obtained by the government, unless certain exceptions apply or if the government has use appropriate legal process with the subscribers or customers being given an opportunity to protect their rights.

Id. at 73.3 The Committee therefore proposed that "individuals have enforceable rights to limit the disclosure of [communications] records maintained about them for third parties," just as they would have the right to limit disclosures of bank or cable records. *Id.* The Court finds that section 2702(a)(3), by prohibiting the disclosures of records to governmental entities, furthers the original purposes of the ECPA.

---

3 The quoted reference to nondisclosure of the "contents of records," in context, concerns records *of the contents* of electronic communications kept in storage by communications providers, not the type of records at issue in this case.

B. AT&T's motion to dismiss

AT&T contends that the *Terkel* plaintiffs have inadequately alleged their standing to sue because they have sufficiently pleaded that their records will be turned over to the government and that AT&T has violated section 2702(a)(3). The plaintiffs respond that they have adequately alleged the facts necessary to establish standing.

First, AT&T argues that the plaintiffs have not adequately alleged that AT&T is disclosing their telephone records to the government. The Seventh Circuit has stated that "'[w]here pleadings concern matters peculiarly within the knowledge of the defendants, conclusory matters peculiarly within the knowledge of the defendants, conclusory pleading on 'information and belief' should be liberally viewed.'" *Brown v. Budz*, 398 F.3d 904, 914 (7th Cir. 2005) (quoting *Tankersley v. Albright*, 514 F.2d 956, 964 n. 16 (7th Cir. 1975)). Because the matters at issue in this case are entirely within the knowledge of AT&T and the government, the *Terkel* plaintiffs have made all of their allegations based upon "information and belief." In their complaint, they have stated the factual bases for their allegations, namely media reports indicating that the government intends to collect and analyze all domestic telephone records, that AT&T has already released large quantities of records, and that federal intelligence gathering agencies have focused on their efforts on large metropolitan areas like Chicago. Am. Compl. ¶¶ 19-25. The Court concludes that under the circumstances, the plaintiffs have sufficiently alleged that they are suffering a particularized injury for which they can seek relief.

Second, AT&T claims that the plaintiffs have not adequately alleged that AT&T's actions have caused them any injury. Plaintiffs correctly point out, however, that they have claimed an ongoing violation of their statutory rights under section 2702(a)(3), an alleged injury

that in itself is sufficient to establish standing. *See Kyles v. J.K. Guardian Sec. Servs., Inc.*, 222 F.3d 289, 298 (7th Cir. 2000) (an individual may establish Article III standing for a statutory violation if she suffers an injury in a form that "the statute was intended to guard against" even though "she has not been harmed apart from the statutory violation"). In addition, unlike the plaintiff in *Kyles*, who alleged only a bare statutory violation, the plaintiffs in this case have gone beyond Article III standing requirements, alleging that AT&T's actions have interfered with their professional relationships. Am. Compl. ¶ 4. The Court concludes that the plaintiffs have adequately alleged that they have suffered a violation of section 2702(a)(3) that is actionable under section 2707.

C. The government's motion to dismiss

The government argues that the Court should dismiss this case or grant summary judgment in AT&T's favor. It contends that the NSA has properly asserted two statutory privileges that bar disclosure of any information about its activities; that prosecution of the litigation would require the government to admit or deny the existence of a secret relationship with AT&T; and that prosecution of the lawsuit would contravene the state secrets privilege, which the government has asserted in its public and *in camera* filings.

The *Terkel* plaintiffs contend that the information needed to prosecute their case does not implicate any of these concerns. Plaintiffs ask the Court to declare that the alleged record disclosure program violates section 2702(a)(3) and to enjoin AT&T from providing customer telephone records to any government agency, absent authorization under Chapter 121 of Title 18 of the United States Code. *Id.* at Part VII. Pending trial on the merits, the *Terkel* plaintiffs have requested a preliminary injunction to this same effect. In aid of their motion for preliminary

injunction, the *Terkel* plaintiffs have filed proposed interrogatories in which they ask AT&T to state whether it has provided or continues to provide customer telephone records to the government; the legal basis, if any, for such disclosures; the number of such disclosures; and the governmental entities to which such disclosures have been made. *See generally*, Pl. Mot. to Permit Ltd. Disc., Ex. 1.

1. Statutory privileges

The government has asserted two statutory privileges in this case: section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note, §6, and section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1). The plaintiffs maintain that neither of these privileges are applicable.

a. Section 6 of the National Security Agency Act

Section 6 provides that:

> [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 persons employed by such agency.

50 U.S.C. § 402 note, § 6. According to the government, because the plaintiffs contend that AT&T has provided customer call information to the NSA, litigating the case would require AT&T to affirm or deny information regarding the activities of the NSA. The government therefore claims that it is entitled to assert the privilege purportedly created by section 6.

The Court has located three decisions, all from the United States Court of Appeals for the D.C. Circuit, discussing the scope of section 6. Each case involved a request for the NSA to release information pursuant to the Freedom of Information Act (FOIA). *See Linder v. Nat'l Sec. Agency*, 94 F.3d 693 (D.C. Cir. 1996); *Founding Church of Scientology of Washington*

D.C., Inc. v. Nat'l Sec. Agency, 610 F.2d 828 (D.C. Cir. 1979); *Hayden v. Nat'l Sec. Agency*, 608 F.2d 1381 (D.C. Cir. 1979). These decisions hold that section 6 gives the NSA the absolute right to withhold from disclosure under FOIA any information covered by section 6. *See Linder*, 94 F.3d at 698; *Hayden*, 608 F.2d at 1389-90; *Founding Church*, 610 F.2d at 828.

In *Hayden*, however, the court reserved deciding whether the NSA could use section 6 to withhold information regarding unauthorized or illegal activities, stating that "where the function or activity is *authorized by statute* and *not otherwise unlawful*, NSA materials integrally related to that function or activity fall within [section 6] and Exemption 3 [of FOIA]." 608 F.2d at 1389 (emphasis added). *Id.* The Court has been unable to locate any later cases discussing this point. We are, however, concerned that if, as the court in *Hayden* anticipated, section 6 is taken to its to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA's functions.

In short, the Court is hard-pressed to read section 6 as essentially trumping every other Congressional enactment and Constitutional provision. Indeed, at oral argument, the government agreed that there is likely a limit to its ability to invoke section 6, though it balked at defining where the line would be drawn, insisting that wherever the line is, this case falls squarely inside it. The Court is skeptical that section 6 is properly read as broadly as the government urges. But because the matters alleged by the plaintiffs are, as we will discuss, subject to the state secrets privilege, we need not definitively determine the thorny issue of the proper scope of section 6.

b. Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004

Section 102A(i)(1) states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from disclosure." 50 U.S.C. § 403-1(i)(1). Plaintiffs concede this statute allows the Director of National Intelligence to withhold information covered by the statute when it is requested of him or agencies under his control. *See, e.g., CIA v. Sims*, 471 U.S. 159 (1985) (holding that precursor to § 102A(i)(1) could shield against FOIA request); *Fitzgibbon v. CIA*, 911 F.2d 755 (D.C. Cir. 1990) (same). In this case, however, the plaintiffs have sued only AT&T and are seeking discovery only from that entity, not the Director of National Intelligence, the NSA, or any governmental agency. Under these circumstances, section 102A(i)(1) does not by itself bar prosecution of this case. Indeed, the statute, by its terms, applies to this case only in that it instructs the Director of National Intelligence to take measures that are available to prevent disclosure regarding intelligence sources and methods – for example, by asserting the state secrets privilege, as Mr. Negroponte has done.

2. Applicability of *Totten/Tenet*

The government also contends that plaintiffs' claims are not justiciable because the very subject matter of their lawsuit is a state secret. Initially, the government argues that plaintiffs' lawsuit concerns an alleged espionage relationship between the government and AT&T. As a result, the government claims that the suit is categorically barred. *See Tenet v. Doe*, 544 U.S. 1 (2005); *Totten v. United States*, 92 U.S. 105 (1876).

The seminal case regarding the justiciability of lawsuits concerning secret espionage contracts is *Totten*, a post-Civil War case in which the estate of a self-identified Union spy sued the government for breach of contract. 92 U.S. at 105. Under the purported contract, the

plaintiff was to obtain intelligence about the Confederacy's troop deployments and fortification efforts in exchange for a two hundred dollar monthly salary; the parties also agreed that the contract's existence and terms would remain a secret. *Id.*. The Supreme Court held that the president undoubtedly had the legal authority to make the alleged contract but that the plaintiff could not pursue a lawsuit to enforce the contract. *Id.* at 106. The Court explained that because acknowledgment of such an agreement or its terms could threaten national security, the estate's claim was not justiciable. *Id*.

The Court recently explained the broad scope of *Totten* in *Tenet*, a case in which two former spies sued the government for constitutional violations based on the government's alleged breach of an espionage agreement they had made with the Central Intelligence Agency. 544 U.S. at 7. The Court cited its statement in *Totten* 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." *Id.* at 8 (quoting *Totten*, 92 U.S. at 107)(emphasis in original)). The Court found that *Totten* applied broadly and therefore concluded that courts could not adjudicate any claims – not just breach of contract actions – by alleged spies based on secret espionage agreements. *Id.* at 7.

According to the government, this case must be dismissed because it would require an inquiry into whether AT&T entered a secret espionage relationship with the government. We assume for the purposes of discussion that the alleged relationship between AT&T and the government, if it exists, constitutes the type of espionage relationship governed by *Totten* and *Tenet*. It is unclear, however, whether those decisions govern this case. The plaintiffs in *Totten* and *Tenet* had entered contracts that they knew were a secret, but they nonetheless attempted to

bring lawsuits to obtain the benefit of their bargain. In contrast, the plaintiffs in this case were not parties to the alleged contract nor did they agree to its terms; rather, they claim that the performance of an alleged contract entered into by others would violate their statutory rights. In addition, while there is no question that the executive branch had the legal authority to enter the contracts in *Totten* and *Tenet*, the plaintiffs have raised a legitimate question as to whether, assuming the alleged agreement with AT&T exists, the President can legally enter into an agreement that would require circumventing the laws of the United States.

At oral argument, the government argued that *Totten* stands for a broader proposition that courts cannot maintain lawsuits that would result in "the disclosure of matters which the law itself regards at confidential." *Id.* at 146-47 (quoting *Totten*, 92 U.S. at 107). In support of its argument, the government cites *Weinberger v. Catholic Action of Haw./Peace Educ. Project*, 454 U.S. 139 (1981). In *Weinberger*, the plaintiff sued the Navy for failure to prepare and publish an environmental impact statement (EIS) regarding the use of a storage facility in Hawaii. The plaintiff claimed that the Navy planned to store nuclear weapons at the facility, a use that could have a significant environmental impact on the surrounding community. Pursuant to regulations adopted to protect national security, the Navy maintained that it could not disclose the planned use for the facility and that it consequently was not required to file an EIS or release one to the public. *Id.* at 140-42.

Having concluded that Navy regulations prohibited disclosure about whether it planned to store nuclear weapons at the facility in question, the Court held the Navy was not required to publish an EIS and that it could not adjudicate the question of whether the Navy had filed an adequate EIS for internal use only. In finding that it could not adjudicate the adequacy of the

internal EIS drafted by the Navy, the Court cited *Totten* for the proposition that courts cannot maintain lawsuits that would result in "the disclosure of matters which the law itself regards at confidential." *Id.* at 146-47 (quoting *Totten*, 92 U.S. at 107).

The government contends that based on *Weinberger*, *Totten* is applicable to any lawsuit in which the subject matter of the case itself is a state secret. This may be true. *But see Tenet*, 544 U.S. at 8-10 (noting that *Weinberger* recognized the continuing validity of *Totten*'s sweeping holding but later describing *Totten* as establishing a categorical bar on "the distinct class of cases that depend upon clandestine spy relationships"). On its face, however, the very subject matter of this lawsuit is not necessarily a state secret. It is obvious that acknowledging the mere existence of a secret espionage relationship or the location of nuclear weapons can jeopardize national security. *See Tenet,* 544 U.S. at 7 (espionage agreements); *Weinberger,* 454 U.S. 146-47 (nuclear weapons storage sites); *Totten,* 92 U.S. at 108 (espionage agreements). Disclosing the mere fact that a telecommunications provider is providing its customer records to the government, however, is not a state secret without some explanation about why disclosures regarding such a relationship would harm national security. Put another way, the Court cannot think of a situation in which publicly acknowledging a covert espionage contract or a secret nuclear weapons facility would not threaten national security. In contrast, the Court can hypothesize numerous situations in which confirming or denying the disclosure of telephone records to the government would not threaten national security and would clearly reveal wholesale violations of the plaintiffs' statutory rights.[4]

---

[4]To use a completely unrelated example, adjudicating this case would not threaten national security if the government were obtaining all customer telephone records from AT&T for the sole purpose of determining the identity of individuals who call psychics. The government could

The Court finds that it would be particularly inappropriate to apply *Totten* to this case. The Supreme Court recently stated that when a case is governed by *Totten*, that decision creates a categorical bar to judicial review. *Tenet*, 544 U.S. at 8. Though the Court ultimately concludes, as discussed below, that this case implicates the state secrets privilege, it has done so only after carefully evaluating the government's claimed justifications. If *Totten* applied to this case, by contrast, it would require outright dismissal without any real judicial review of whether this case in fact implicates state secrets.

3. The state secrets privilege

The government's primary argument is that assertion of the state secrets privilege bars the making of responses to the *Terkel* plaintiffs' proposed interrogatories and, indeed, precludes the *Terkel* plaintiffs from establishing their standing to sue or from establishing a right to relief against AT&T. The state secrets privilege is a common law evidentiary privilege that allows the government to "block discovery of any information that, if disclosed, would adversely affect national security." Because the privilege, if applicable, is absolute, its successful assertion may be fatal to the underlying case. *Ellsberg v. Mitchell*, 709 F.2d 51, 56 (D.C. Cir. 1983). Proper assertion of the privilege makes the information at issue unavailable, often rendering a plaintiff unable to establish a *prima facie* case and without a remedy for the violation of her rights. *Id.* For these reasons, courts have warned that "'[the privilege] is not to be lightly invoked.'" *Id.* (quoting *United States v. Reynolds*, 345 U.S. 1, 7 (1953)).

---

not claim that affirming or denying such a program would threaten national security because it would enable psychics to avoid detection by the government.

The leading Supreme Court case addressing the state secrets privilege is *Reynolds*, which involved the crash of an Air Force bomber. Three of the four civilians aboard the bomber died in the accident, and their widows sued the United States under the Federal Tort Claims Act. The plaintiffs sought discovery of an Air Force investigation report regarding the crash. The government asserted the state secrets privilege, claiming that release of the report would threaten national security interests. Specifically, the government stated that the bomber was testing secret electronic equipment and that the report contained classified information about the equipment. *Reynolds*, 345 U.S. at 2-5.

The Court in *Reynolds* explained that the state secrets privilege traced its origins to English common law. *Id.* at 7. The Court noted that it was first invoked in the United States during the treason trial of Aaron Burr but that the privilege had been discussed by few courts since then. *Id.* Drawing on these cases, the Court enumerated the formal requirements for asserting the privilege, concluding that only the government, and not private parties, may assert or waive the state secrets privilege. More specifically, the head of the department that oversees the information in question must assert the privilege formally after personally considering the matter. *Id.* at 7-8.

The Court also explained the judiciary's role in evaluating an executive official's assertion of the privilege. The Court made it clear that "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." *Id.* at 9-10. Courts must determine "whether the circumstances are appropriate for the claim of privilege" but must do so "without forcing the disclosure of the very thing the privilege is designed to protect." *Id.* at 8.

The depth of a court's inquiry into the propriety of the invocation of the state secrets privilege depends on the circumstances of the case. "Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted...[but] where necessity is dubious, a formal claim of privilege, made under the circumstances of this case, will have to prevail." *Id.* at 11. However, "even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake."[5] *Id.* The Court ultimately concluded that the Air Force had properly asserted the privilege with regard to the investigation report. It declined, however, to dismiss the plaintiffs' case as they had alternate means of establishing the cause of the crash. *Id.* at 12.

In this case, it is undisputed that the government has complied with the formal requirements for invoking the privilege. *See Reynolds*, 345 U.S. at 7-8. Mr. Negroponte has filed in the public record a declaration formally asserting the privilege on behalf of the government. Negroponte Decl. ¶ 3. Specifically, Mr. Negroponte has, in his public declaration, invoked the privilege as to:

> any information tending to confirm or deny (a) alleged intelligence activities, such as the alleged collection by the NSA of records pertaining to a large number of telephone calls, (b) an alleged relationship between the NSA and AT&T (either in general or with respect to specific alleged intelligence activities), and (c) whether particular individuals or organizations have had records of their telephone calls disclosed to the NSA.

---

5 The D.C. Circuit has held, and this Court agrees, that the privilege covers not just "military secrets" as such, but information whose release could lead to "the impairment of the nation's defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign governments." *Ellsberg*, 709 F.2d at 57.

Negroponte Decl. ¶ 11. Lieutenant General Keith Alexander, the Director of the NSA, has also filed a public declaration supporting Mr. Negroponte's assertion of the privilege. Alexander Decl. ¶ 2.

For their part, the *Terkel* plaintiffs have made a strong showing of necessity for the information over which the government claims the privilege. The necessity requirement articulated in *Reynolds* incorporates two related but distinct concepts: whether the information at issue is essential to the case, and whether it is available through alternate means. *See Reynolds*, 345 U.S. at 11; *Northrop Corp. v. McDonnell Douglas Corp.*, 751 F.2d 395, 399 & 401 n. 7 (D.C. Cir. 1984). In this case, the plaintiffs have established both types of necessity: they need the information as to which the privilege is claimed to establish their standing and a *prima facie* case, and they have been unable to point to any other available sources for the information they need. For these reasons, "the claim of privilege cannot be lightly accepted." *Id.* at 11.

The question before the Court, therefore, is whether the government has shown that based on the circumstances of the case and the interrogatories posed by the plaintiffs, "'responsive answer[s] to the question[s] or [] explanation[s] of why [they] cannot be answered might be dangerous because injurious disclosure could result.'" *Id.* at 9 (quoting *Hoffman v. United States*, 341 U.S. 479, 486-87 (1951) (identifying circumstances under which to allow invocation of Fifth Amendment privilege against self-incrimination)).

The *Terkel* plaintiffs claim that AT&T violated section 2702(a)(3) by unlawfully disclosing their telephone records to the government. They have posed seven interrogatories to AT&T in an attempt to develop the factual basis for their claims. As discussed above, the

plaintiffs ask AT&T to disclose whether it has knowingly and/or intentionally provided customer telephone records to the federal government and to identify the federal government entities to which these disclosures have been made, the quantity of records disclosed, the legal basis, if any, for the disclosures, and whether AT&T is disclosing such records at present.

Plaintiffs contend that the answers to these questions do not implicate state secrets. Rather, they maintain that they only need information about "very general intelligence techniques" that are already public knowledge, the disclosure of which will not reveal to enemies of the United States "the fact that surveillance of [their] activities has occurred, the targets and extent of such surveillance, or the means by which it was accomplished." *See ACLU v. Brown*, 619 F.2d 1170, 1174 (7th Cir. 1980) ("*ACLU II*"). Plaintiffs further maintain that the answers to the limited questions they have posed would be sufficient to allow them to prosecute their case. Pl. Resp. at 9-10.

The government disagrees. In his publicly filed declaration, Mr. Negroponte maintains that the government cannot confirm or deny information regarding its intelligence activities because any disclosure would threaten national security. Negroponte Decl. ¶ 12. He states that confirming any activities would compromise intelligence sources and enable adversaries, including members of Al Qaeda, to avoid detection. *Id.* He further states that:

> [e]ven confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels, would cause harm to the national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection.

Id. Finally, Mr. Negroponte maintains that "denying false allegations is an untenable practice" as adversaries could deduce important information about American intelligence practices based

on the government's denial of certain claims and failure to respond to others. Negroponte Decl. ¶ 12.

The government has also filed additional materials *in camera* and *ex parte* further justifying its invocation of the state secrets privilege. Specifically, the government's public submissions disclose that it has filed additional declarations from Lt. Gen. Alexander and Mr. Negroponte that contain classified information. The government has also filed an *in camera*, *ex parte* version of its brief that discusses the *in camera* declarations and additional reasons why the Court should uphold the assertion of the state secrets privilege. The Court has reviewed these submissions thoroughly. After doing so, we questioned government counsel, *in camera* and *ex parte*, about certain aspects of the submissions and requested further information, which the government later provided. The Court cannot disclose the contents of the *in camera* submissions, as we cannot divulge "the very thing the privilege is designed to protect." *See Reynolds*, 345 U.S. at 8. As noted earlier, we have issued a separate Memorandum addressing the *in camera* submissions. The present, publicly issued Memorandum Opinion does not take the *in camera* submissions into account but rather is based entirely on the public record.

Because the government's *in camera* submissions were made, and were required to be made, *ex parte*, the plaintiffs have been unable to examine some of the information supporting the government's assertion of the state secrets privilege. They argue, however, that the information they need to prosecute their case is already in the public domain and therefore is not subject to the state secrets privilege. In support of their argument, the *Terkel* plaintiffs cite several newspaper articles asserting that AT&T has provided large quantities of telephone records to the federal government, specifically the NSA, without statutory authorization. Susan

Page, *Lawmakers: NSA Database Incomplete*, U.S.A. Today, June 30, 2006, at 2A (hereinafter, "U.S.A. Today, June 30, 2006"); Jon Van and Michael O'Neal, *Phone Giants Raise Doubts on NSA Story*, Chic. Trib., May 17, 2006, at 1 (hereinafter, "Chic. Trib., May 17, 2006"); Eric Lichtblau, *Bush Is Pressed Over New Report On Surveillance*, N.Y. Times, May 12, 2006, at A1; Barton Gellman, *Data On Phone Calls Monitored*, Wash. Post, May 12, 2006, at A1; Lesley Cauley, *NSA Has Massive Database Of Americans' Phone Calls*, U.S.A. Today, May 11, 2006, at 1A (hereinafter, "U.S.A. Today, May 11, 2006"); Josh Meyer, *U.S. Spying is Much Wider, Some Suspect*, L.A. Times, Dec. 26, 2005, at 1; Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times, Dec. 24, 2005, at A1.

Plaintiffs also focus the court's attention on statements by other telephone companies, including Bell South, Qwest, and Verizon, denying that they provide large quantities of telephone records to the government. Specifically, Bell South and Verizon have indicated that they have not engaged in the wholesale disclosure of customer telephone records to the government. *See* BellSouth, *BellSouth Statement on Government Data Collection*, May 15, 2006, available at http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860&printable ("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."); Verizon, *Verizon Issues Statement on NSA and Privacy Protection*, May 12, 2006, available at http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93446&PROACTIVE_ID=cecdc6c9c7cfcdc7c7c5cecfcfcfc5cecdcec9c7c6cccec7c9c5cf ("Verizon does not, and will not, provide any government agency unfettered access to our customer records or provide

information to the government under circumstances that would allow a fishing expedition.").[6] Qwest, another communications provider, has been even more specific in its disclosures. According to counsel for Qwest's former Chief Executive Officer Joseph Nacchio, the government approached Mr. Nacchio several times between fall of 2001 and summer of 2002 to request its customer telephone records, but because the government failed to cite any legal authorization in support of its demands, Mr. Nacchio refused the requests. *See* John O'Neil, *Qwest's Refusal of N.S.A. Query Is Explained*, N.Y. Times, May 12, 2006. AT&T, in contrast, has stated only that when it does release records to the government, it does so in accordance with all laws and regulations. AT&T, *AT&T Statement on NSA Issue*, June 27, 2006, available at http://att.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22372 ("What we can say is AT&T is fully committed to protecting our customers' privacy and would not provide customer information to any government agency except as specifically authorized under the law.").

Plaintiffs also point to the government's official acknowledgment of a program to monitor the contents of telephone calls. *See, e.g.,* Department of Justice, *Legal Authorities Supporting the Activities of the NSA Described by the President* (Jan. 19, 2006) (admitting existence of content-monitoring program and explaining legal basis for the program). Specifically, President Bush and Attorney General Gonzales stated publicly that the government intercepts communications in which one party to the conversation is a suspected member of Al Qaeda, regardless of whether the communications involve parties in the United States. *See*

---

6 Based on the wording of Verizon's press release, it is unclear whether the telephone company MCI engaged in such conduct prior to its acquisition by Verizon earlier this year. *See* Verizon Press Release.

Hepting, slip op. at 19-21 (collecting press releases). The *Terkel* plaintiffs concede, however, that no executive branch official has officially confirmed or denied the existence of any program to obtain large quantities of customer telephone records, the subject of the plaintiffs' lawsuit.

Based on these media reports and official admissions, the *Terkel* plaintiffs argue that the activities alleged in the complaint are not state secrets because they are publicly known and, further, that adversaries of the United States surely know about these activities and have already adjusted their behavior accordingly. The government strenuously denies the plaintiffs' contentions. It maintains that neither AT&T nor the executive branch of the government has confirmed or denied allegations that AT&T has disclosed large quantities of consumer telephone records. It also contends that requiring AT&T to affirm or deny these allegations would harm national security by arming adversaries of the United States with more concrete knowledge about how best to use communications channels to achieve their violent goals. In particular, the government argues, enemy groups could utilize a confirmation or a denial of the activities at issue in this case to assess the relative risks of using particular providers and to avoid detection of their communications. Specifically, if they learned that AT&T was disclosing telephone records, they might use another provider to avoid surveillance of their activities; if they learned that AT&T had withheld such records from the government, they might switch to AT&T.

The question the Court must determine is whether the information sought by the plaintiffs is truly a secret or whether it has become sufficiently public to defeat the government's privilege claim. Ascertaining whether alleged activities that have been discussed in the public

domain remain state secrets is a difficult task, particularly because few courts have thoroughly addressed the issue.[7]

It seems logical, however, that the focus should be on information that bears persuasive indication of reliability. In particular, public admissions by the government about the specific activity at issue ought to be sufficient to overcome a later assertion of the state secrets privilege. Judge Walker relied on such disclosures in *Hepting* when he concluded that the existence of a program of monitoring the contents of certain telephone communications was no longer a state secret as a result of the recent public statements by the President and the Attorney General. *Hepting*, slip op., at 19-21, 28.

Similarly, admissions or denials by private entities claimed to have participated in a purportedly secret activity may, under appropriate circumstances, constitute evidence supporting a contention that the state secrets privilege cannot be claimed as to that particular activity. As is the case with official governmental disclosures, such statements reasonably may be considered reliable because they come directly from persons in a position to know whether or not the

---

7 We have been unable to locate any appellate decisions that squarely address the question of when press reports may be considered to have divulged what would otherwise constitute state secrets. The seminal appellate court cases on the state secrets privilege address the question of whether the government, once it has officially released some information about intelligence activities, must release additional information about those activities. *See Ellsberg*, 709 F.2d at 59-60 (concluding that government, having acknowledged conducting surveillance of certain plaintiffs, could nonetheless invoke the state secrets privilege as to whether other plaintiffs had been subjected to surveillance); *Halkin I*, 598 F.2d at 9 (concluding that the government, having acknowledged conducting surveillance of an individual in one case, could nonetheless assert state secrets privilege as to whether plaintiff in *Halkin I* had been subjected to surveillance). These cases are of limited assistance here, however, because they do not address the question of whether alleged intelligence activities are no longer secrets because the media has issued reports about them.

supposedly covert activity is taking place. Again, Judge Walker relied on disclosures of this type in his decision in *Hepting*. *See Hepting*, slip op. at 21-23, 29-32.

As the *Terkel* plaintiffs concede, however, neither AT&T nor the government has made any statements confirming or denying AT&T's participation in the particular program alleged in this case.[8] As a result, the existence of the activities at issue has not become public knowledge based on any statements by those entities that are most likely to have personal knowledge about the matters at issue.

The *Terkel* plaintiffs insist that the press reports discussed earlier are sufficient to render their allegations matters of public knowledge. The Court disagrees. The plaintiffs initially argue that this case is controlled by *Spock v. United States*, 464 F. Supp. 510, 520 (S.D.N.Y. 1978), in which the plaintiff alleged that government agents unlawfully intercepted his electronic communications. *See id.* at 512. The court concluded that the state secrets privilege did not apply because the press had widely reported that the plaintiff had been under government surveillance. *Id.* at 520. Plaintiffs cite *Spock* for the proposition that media reports about intelligence activities make those activities public knowledge, rendering the state secrets privilege inapplicable. *See id.*

---

8 In *Hepting*, the plaintiffs cited an equivocal statement by AT&T which arguably suggested that it may be assisting the government with surveillance. *Id.* at 30-31 (citing News Release, *AT&T Statement on Privacy and Legal/Security Issues* (May 11, 2006), available at http://www.sbc.com/gen/press-room?pid=4800&cdvn+news&newsarticleid=22285 ("If and when AT&T is asked to help, we do so strictly within the law and under the most stringent conditions.")). This statement offers no indication, however, that the means of any such assistance by AT&T consists of the wholesale disclosure of customer telephone records.

The Court disagrees with the analysis in *Spock* and therefore declines to apply it to this case. Indeed, as the government pointed out at oral argument, it would undermine the important public policy underlying the state secrets privilege if the government's hand could be forced by unconfirmed allegations in the press or by anonymous leakers whose disclosures have not been confirmed. Neither the media reports cited here, nor those in *Spock*, are the result of official disclosures, nor is there any way for the Court to say that they are based on information from persons who would have reliable knowledge about the existence or non-existence of the activity alleged. Rather, on the present record at least, these reports amount to nothing more than unconfirmed speculation about the particular activity alleged in this case. *Accord, Hepting*, slip op. at 25. As a result, the Court cannot treat them as making the alleged activities at issue in this case matters of public knowledge.

The *Terkel* plaintiffs have also cited one press report indicating that executive officials briefed members of Congressional Intelligence Committees in closed-door sessions about the activities at issue here. *See* U.S.A. Today, June 30, 2006. The article states that five unnamed members of the committees stated that "they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program." *Id.* Based on this article, plaintiffs argue that the Court should follow *Jabara v. Kelley*, 75 F.R.D. 475, 493 (E.D. Mich. 1977), a case in which the plaintiff claimed that multiple government agencies had conducted unconstitutional surveillance of his activities. The plaintiff sought to discover the identities of those agencies. The court held that the identity of one unnamed agency had ceased to be a state secret once the agency had been named in a Congressional report. *Id.* Plaintiffs cite *Jabara* for

the notion that once executive officials have disclosed certain activities to members of Congress, those activities are no longer covered by the state secrets privilege.

It is unclear from the decision in *Jabara* whether executive officials disclosed the information in the Congressional report in a public or private setting. If it was the latter, the Court disagrees with *Jabara*. Treating confidential statements to Congressional representatives as public disclosures that make an otherwise secret activity a matter of public knowledge would undermine the state secrets privilege by forcing the executive branch to give up the privilege whenever it discusses classified activities with members of Congress. Just as importantly, it would also discourage executive officials from candidly discussing intelligence activities with Congress, further reducing the legislative branch's ability to hold executive officials accountable. If, on the other hand, the revelations by the executive officials in *Jabara* were made in a public setting, the case is inapposite; there is no indication of any such public disclosure relevant to the allegations in this case.

Our conclusion is supported by case law interpreting the Freedom of Information Act. *See ACLU v. Brown*, 609 F.2d 277, 280 (7th Cir. 1979) ("*ACLU I*") (finding FOIA case law instructive in ascertaining the applicability of the state secrets privilege).[9] FOIA allows individuals to obtain documents held by the government, 5 U.S.C. § 552(a)(2), but it creates an exemption for documents that are shielded from disclosure by statute. 5 U.S.C. § 552(b)(3). A

---

9 The plaintiffs discourage us from invoking FOIA case law to ascertain what constitutes information in the public domain. They argue that determining whether the government is entitled to an exemption from disclosure is a much narrower inquiry than whether the government is entitled to invoke the state secrets privilege as to matters that arise in litigation. That may be so. The Court nonetheless finds the policy considerations expressed in the FOIA jurisprudence helpful to the extent they deal with the general question of how to determine whether a matter claimed to implicate national security interests is publicly known.

petitioner under FOIA may nonetheless overcome this exemption by showing that the agency invoking it has officially and publicly acknowledged the requested information. *See Fitzgibbon*, 911 F.2d at 765.

FOIA case law is clear, however, that unconfirmed media reports about an alleged governmental activity are insufficient to render information public knowledge. *See Fitzgibbon*, 911 F.2d at 765 ("'It is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so.'") (quoting *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975)). As the court stated in *Afshar v. Dep't of State*, 702 F.2d 1125, 1130, 33-34 (D.C. Cir. 1983), "[e]ven if a fact...is the subject of widespread media and public speculation, its official acknowledgment by an authoritative source might well be new information that could cause damage to the national security." A disclosure must be both official and public for the fact at issue to be considered a matter of public knowledge for FOIA purposes. *See Fitzgibbon*, 911 F.2d at 765.

As noted earlier, the plaintiffs contend that the alleged program at issue in this case cannot be a state secret because of disclosures made by other telecommunications companies. Two such companies, Bell South and Verizon, have flatly denied making such disclosures. Judge Walker also considered these arguments in *Hepting*. *See Hepting*, slip op. at 21-23 (citing press releases from Bell South, Verizon, and Qwest). The plaintiffs also point to another news report quoting counsel for the former chief executive officer of Qwest, who (as discussed earlier) stated that the government approached the CEO about obtaining access to telephone records, but he refused after learning that the government lacked legal authority supporting its request. *See*

John Markoff, *Questions Raised for Phone Giants in Spy Data Furor*, N.Y. Times, at A1, May 13, 2006. The plaintiffs hypothesize that if Bell South's, Qwest's, and Verizon's denials did not reveal state secrets, confirmation or denial of AT&T's participation in the alleged program would not reveal state secrets either.

The Court disagrees. Initially, the Court fails to see how the statements by Bell South and Verizon, in which they simply deny the allegations without elaboration, can be considered to have disclosed the existence or non-existence of the program alleged by the *Terkel* plaintiffs. The statement by the former Qwest executive comes somewhat closer to the mark. But plaintiffs' reliance on that disclosure misses the point. Their case concerns AT&T, not any other telephone companies. Requiring AT&T to admit or deny the existence of a request by the government as to AT&T, or AT&T's response if a request was made, would disclose significant information that has not been made public by anything the Qwest executive reported. This is so even if one were to infer from that report that the government had some sort of program in place: admitting or denying an approach to AT&T, or its response if an approach was made, would reveal information about the scope of the claimed program that could impact national security. Specifically, such a disclosure or a denial could permit would-be terrorists to tailor their activities to avoid detection. In addition, as Judge Walker stated in *Hepting*:

> 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.

Hepting, slip op. at 40-42.

The *Terkel* plaintiffs have brought to our attention Judge Walker's decision in *Hepting*, arguing that it supports denial of the government's privilege claim in this case. But the *Terkel* case (unlike, perhaps, the others assigned to this Court, *Joll* and *Waxman*) differs from *Hepting*. The differences are significant, and they lead this Court to a result different from the one Judge Walker reached. The plaintiffs in *Hepting* challenged, among other things, the alleged interception of the *contents* of communications by the NSA with AT&T's assistance – a challenge not made in *Terkel*. Judge Walker concluded that public disclosures by the government of a "terrorist surveillance program" involving interception of communications contents, along with other factors, made that particular alleged program, AT&T's possible participation in it, and the existence of any assurances of legality by the government no longer secrets that are protected by *Totten* or the state secrets privilege. *See Hepting*, slip op. at 29-31 (discussion of *Totten*), 35 & 39 (discussion of the state secrets privilege claim). The *Terkel* plaintiffs, however, currently advance no claim about content monitoring.

Hepting also includes claims based on AT&T's alleged disclosure to NSA of telephone call records – the same claims (indeed the only claims at this juncture) made by the *Terkel* plaintiffs. Judge Walker expressed some skepticism as to whether the existence or non-existence of such a program is a state secret, in light of the disclosures of the "terrorist surveillance program" and denials by other companies that they participated in a program of disclosure of call records. *See Hepting*, slip op. at 40-41. In the final analysis, however, Judge Walker concluded, as we do, that at present at least, the potential for risk from disclosure of the existence or non-existence of such a program, or AT&T's involvement or non-involvement, made it imprudent to

require such disclosures. As a result, he declined to permit discovery about those particular allegations. *See id.* at 41-42.

Where that conclusion leads this Court is affected by the differences between this case and *Hepting*. Judge Walker determined, in effect, that because the allegations regarding the publicly-revealed *content* monitoring activity could proceed, there was no basis to dismiss or otherwise terminate the claims about the alleged *record* monitoring activity. *See id.* at 42, 50. Specifically, Judge Walker indicated that as the claims about content monitoring proceeded, further disclosures might be made (in the case or otherwise) that would remove the allegations about record disclosure from the protection of the state secrets privilege. *See id.* Thus he saw no need to dismiss the latter allegations at present. This Court does not necessarily agree with that particular aspect of Judge Walker's decision, but even were we to agree, this would have no bearing on the *Terkel* case. In *Terkel*, the *only* claims in the plaintiffs' amended complaint are those arising from the alleged record disclosure activity. Thus our determination that discovery on those allegations cannot proceed – a point on which this Court and Judge Walker effectively agree – effectively brings to a halt all of the discovery requested by the *Terkel* plaintffs.

In sum, based on the government's public submission, the Court is persuaded that requiring AT&T to confirm or deny whether it has disclosed large quantities of telephone records to the federal government could give adversaries of this country valuable insight into the government's intelligence activities. Because requiring such disclosures would therefore adversely affect our national security, such disclosures are barred by the state secrets privilege. The Court reaches this conclusion based on the government's public submission, without reference to its classified *ex parte* submissions. We do not discuss in this decision any of the

material contained in the classified submissions. We can state, however, that we have rejected some of the claims made by the government in those submissions and have expressed skepticism about others. Those particular matters aside, however, the remainder of the classified submissions provide support for the conclusions the Court has reached based on the government's public submission. As noted earlier, the Court has prepared a classified Memorandum discussing the results of our review of the *in camera* material.

Having concluded that the government has properly invoked the state secrets privilege with regard to any information tending to confirm or negate the factual allegations presented in the *Terkel* plaintiffs' complaint, the final question is whether the Court should allow the case to proceed. The government argues that because the *Terkel* plaintiffs can neither establish standing nor a *prima facie* case without the information subject to the state secrets privilege, the Court should dismiss the case or grant summary judgment. Plaintiffs respond that dismissal or summary judgment at this stage would be an extreme remedy; they contend that we should modify ordinary rules of procedure and/or burdens of proof to enable them to prosecute their case. *See Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1238 n. 3 (4th Cir. 1985) (stating in dicta that "[o]ften, through creativity and care, [the] unfairness caused [by assertion of the state secrets privilege] can be minimized through the use of procedures which will protect the privilege and yet allow the merits of the controversy to be decided in some form," but ultimately declining to modify ordinary procedures because subject matter of lawsuit was a state secret).

Plaintiffs offer several proposals for how they might maintain this lawsuit while allowing protection of state secrets, such as applying a presumption arising from the loss of evidence, *see Halkin v. Helms*, 690 F.2d 977, 991 (D.C. Cir. 1982) ("*Halkin II*"); conducting an *in camera*

trial, *see Halpern v. United States,* 258 F.2d 36, 41 (2d Cir. 1958); entering strict protective orders, *see DTM Research, L.L.C. v. AT&T Corp.*, 245 F.3d 327, 333-35 (4th Cir. 2001); taking depositions in secure facilities; *see In re Under Seal*, 945 F.2d 1285, 1287 (4th Cir. 1991); adding an attorney to plaintiffs' legal team who has security clearance or granting security clearance to one of plaintiffs' current counsel, *cf. Al Odah v. United States*, 346 F. Supp. 2d 1, 14 (D.D.C. 2004); *In re Guantanamo Detainee Cases*, 344 F. Supp. 2d 174, 179-80 (D.D.C. 2004); or appointing a special master. *Cf. Loral Corp. v. McDonnell Douglas Corp.*, 558 F.2d 1130, 1132 (2d Cir. 1977).

The problem with most of plaintiffs' proposals is that in those cases where the government has invoked the state secrets privilege and the court made modifications to the ordinary rules of procedure, it did so to allow for the introduction of classified information that *did not* constitute a "state secret" protected by the state secrets privilege. *See Halpern*, 258 F.2d at 43 (allowing *in camera* trial by inventor of secret invention against the government so long as state secrets not divulged); *DTM Research, L.L.C.*, 245 F.3d at 333-35 (entering protective order over state secrets but allowing case to proceed based on evidence that did not constitute a state secret); *In re Under Seal*, 945 F.2d at 1287 (allowing depositions at secured facilities with government officials present to ensure state secrets not revealed). In the instant case, by contrast, the Court has already concluded that the state secrets privilege covers any disclosures that affirm or deny the activities alleged in the complaint. As a result, the information at issue is unavailable in its entirety, as a result the alternative procedures used in these cases cannot be utilized here.

The *Terkel* plaintiffs alternatively propose altering the standard of proof for proving standing, as well as the existence of a *prima facie* case on the merits, by adopting presumptions favoring them due to their inability to obtain the evidence they need. The plaintiffs cite *Halkin II* in support of this approach. In *Halkin II*, the court suggested in *dicta* that changing procedural rules "could compensate the party 'deprived' of his evidence by, for example, altering the burden of persuasion upon particular issues, or by supplying otherwise lost proofs through the device of presumptions or presumptive inferences." *See Halkin II*, 690 F.2d at 991. The court declined to do so in that case, however, because it had declined to alter the parties' burdens in an earlier ruling in the same case. *Id.* (citing *Halkin I*, 598 F.2d at 11).

The Court has been unable to locate any cases in which courts have decided to alter burdens of proof to neutralize the effect of the successful invocation of the state secrets privilege. Indeed, in *Ellsberg,* the D.C. Circuit appears to have abandoned its *dicta* from *Halkin II*, concluding that "the result [of the government's successful invocation of the state secrets privilege] is simply that the evidence is unavailable, as though a witness has died, and the case will proceed accordingly, with no consequences save those resulting from the loss of the evidence.'" *Ellsberg*, 709 F.2d at 64 (quoting McCormick's Handbook of the Law of Evidence 235 (E. Cleary ed. 1972)). The Court is convinced that this rule is correct, particularly in cases where the government, a non-party, has intervened to assert the state secrets privilege over information requested from one of the parties to the case. "In such a case, sanctions against a party are inappropriate because neither party is responsible for the suppression of the evidence." *See Farnsworth Cannon, Inc. v. Grimes,* 635 F.2d 268, 271 (4th Cir. 1980) (quoting 2 J. Weinstein & M. Berger, Weinstein's Evidence ¶ 509(10) (1979)). In this case, because the

government intervened to assert the privilege, it would be unfair to AT&T to ease the plaintiffs' burden of proof based on decisions beyond its control.

The plaintiffs point out that "[t]he privilege may not be used to shield material not strictly necessary to prevent injury to national security; and whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter." *Ellsberg*, 709 F.2d at 57. Thus, when the government asserts the state secrets privilege as to a wide range of requested disclosures, "the District Court's inquiry must look at each item or logically related group of items individually in order to assure full consideration of the government's claims." *ACLU I*, 609 F.2d at 280. The Court is satisfied, having carefully reviewed the government's public submission, that at the very least, requiring AT&T to admit or deny the core allegations necessary for the plaintiffs to prove standing – whether *their* information is being disclosed – implicates matters whose public discussion, be it an admission or a denial, could impair national security.

The Court has also considered, as an alternative, whether requiring AT&T to answer more generalized questions would avoid implicating the state secrets privilege. Some examples of such questions might be whether AT&T has disclosed *any* of its customers' records to the federal government; whether it has ever done so without statutory authorization or proper justification; and whether it has ever done so with regard to the telephone records of any of the named plaintiffs. The problem, however, is that such generalized answers would not allow the

named plaintiffs to establish standing to seek injunctive relief – the only relief they seek[10] – either on behalf of themselves or a class.[11]

To obtain prospective relief, the plaintiffs must show that there is a "real or immediate threat" that AT&T will, in the future, violate their rights under section 2702(a)(3). *See City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983). In *Lyons*, the plaintiff had sued the Los Angeles Police Department to enjoin the practice of using chokeholds absent the threat of deadly force. *Id.* at 98. The Supreme Court concluded that although the plaintiff had been subjected to this practice on a prior occasion and at least sixteen people in Los Angeles had died from the practice, the plaintiff had failed to establish that he had standing to seek injunctive relief. *Id.* at 97-98, 100. Drawing on its decision in *O'Shea v. Littleton*, 414 U.S. 488 (1974), the Court reiterated that "[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief ... if unaccompanied by any continuing, present adverse effects." *Id.* at 102 (quoting *O'Shea*, 414 U.S. at 495-96). Though "[p]ast wrongs [are] evidence bearing on 'whether there is a real and immediate threat of repeated injury,'" *id.* at 102 (quoting *O'Shea*, 414 U.S at 496), the Court in *Lyons* concluded that the plaintiff lacked standing to seek prospective relief because even if he could prove that he was likely to be arrested again, he would have to prove "(1) that *all* police officers in Los Angeles *always* choke any citizen with whom they happen to have an encounter, whether for the purpose of arrest, issuing a citation or

---

10 Ordinarily, a court may grant appropriate relief to a plaintiff whether he seeks it or not. *See* Fed. R. Civ. P. 54(c). But in this case, the plaintiffs advised the Court both prior to and during oral argument that in their current complaint, they seek only prospective relief and not damages for past alleged violations.

11 The Court also notes that the plaintiffs have cited no authority that would allow us to modify the standards for proving standing under Article III.

for questioning or, (2) that the City ordered or authorized police officers to act in such manner." *Id.* at 106 (emphasis in original).

By successfully invoking the state secrets privilege, the government has foreclosed discovery that would allow the plaintiffs to attempt to establish that they are suffering ongoing harm or will suffer harm in the future. First, the *Terkel* plaintiffs cannot establish whether AT&T has unlawfully disclosed their records in the past, a fact which would allow them to sue for prospective relief if they could also show they are suffering "continuing, present adverse effects." *Id.* at 102 (quoting *O'Shea*, 414 U.S. at 495-96). Second, the plaintiffs cannot establish whether AT&T is currently disclosing their records, which would tend to show that there is a real and immediate threat of repeated injury. *Id.* (quoting *O'Shea*, 414 U.S at 496).

The thrust of plaintiffs' claim is that AT&T shares *all* of its customer telephone records with the government and that as a result, the plaintiffs are among the persons who have suffered and will continue to suffer the harm that flows from such disclosures. Standing doctrine normally allows courts to adjudicate such claims: though the harm impacts a wide class of people, each member of the class has suffered a particularized injury. *See FEC v. Akins*, 524 U.S. 11, 23 (1998) (concluding that standing doctrine only bars adjudication of such cases "where the harm at issue is not only widely shared, but is also of an abstract and indefinite nature"). The problem in this case, however, is that the state secrets doctrine bars the disclosure of matters that would enable the *Terkel* plaintiffs to establish standing in this manner, specifically whether or not AT&T discloses or has disclosed *all* of its customer records to the government, or whether or not it discloses or has disclosed the named plaintiffs' records specifically. *See Halkin II*, 690 F.2d at 998-1003.

The named plaintiffs' inability to establish standing on their claims for prospective relief is fatal to their claims as representatives of a putative class. It is clear that the named plaintiffs in a class action must establish standing individually to serve as class representatives; the *Terkel* plaintiffs do not contend otherwise. *See Warth v. Seidlin*, 422 U.S. 490, 502 (1975) (named plaintiffs seeking to represent a class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent."). Thus, even were AT&T to answer whether it had disclosed to the government the telephone records of some of its customers, none of the named plaintiffs would be able to establish standing, because they still could not establish a personal injury. *See id.*

The Court has great antipathy for dismissing a claim at the pleading stage in a case in which the plaintiffs claim they have suffered a violation of their rights. But "[a]bsent the presence of an identifiable party whose claim of injury can be evaluated on its particular facts, the contentions raised here are simply a request for an advisory opinion" that the federal courts cannot entertain. *Halkin II*, 690 F.2d at 1003 n.6. Nothing in this opinion, however, prevents the plaintiffs from using of the legislative process, not to mention their right to free speech, to seek further inquiry by the executive and legislative branches into the allegations in their complaint. In short, though the *Terkel* plaintiffs cannot seek relief in court for the claims made in their complaint as it now stands, they are free to seek redress from the political branches, which are equally responsible to ensure that the law is followed.

Conclusion

For the reasons stated above, the Court denies AT&T's motion to dismiss [docket no. 39] and grants the government's motion to dismiss [docket no. 48]. The *Terkel* plaintiffs' complaint is dismissed, with leave to amend on or before August 1, 2006 if they wish to do so. The case, along with the *Joll* and *Waxman* cases, is set for a status hearing on August 3, 2006 at 9:30 a.m.

MATTHEW F. KENNELLY
United States District Judge

Date: July 25, 2006