ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (Bar No. 145997)
cindy@eff.org
LEE TIEN (Bar No. 148216)
tien@eff.org
KURT OPSAHL (Bar No. 191303)
kurt@eff.org
KEVIN S. BANKSTON (Bar No. 217026)
bankston@eff.org
CORYNNE MCSHERRY (Bar No. 221504)
corynne@eff.org
JAMES S. TYRE (Bar No. 083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL and ERIK KNUTZEN, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, vs. AT&T CORP., et al. Defendants.	No. C-06-00672-VRW CLASS ACTION PLAINTIFFS' OPPOSITION TO MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA BASED ON THE STATE SECRETS PRIVILEGE Judge: The Hon. Vaughn R. Walker Date: June 23, 2006 Courtroom: 6, 17th Floor

REDACTED PUBLIC VERSION

TABLE OF CONTENTS

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES **Page**

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

STATUTES

TABLE OF AUTHORITIES

OTHER AUTHORITIES

RULES

INTRODUCTION

For at least the past three years, AT&T has engaged in the wholesale illegal interception and disclosure to the NSA of its customers' personal communications and records. These actions violate no less than four federal statutes, each of which provides for a civil cause of action for illegal surveillance. They have been undertaken without regard to the judicially-controlled processes for supervising the executive's need to protect national security. And they do not constitute state secrets. For even without the benefit of the ordinary judicial discovery processes, plaintiffs have already presented a *prima facie* case on each cause of action using admittedly non-classified evidence.

Yet despite the settled statutory framework and the private rights of action established by Congress, and notwithstanding the non-secret record evidence supporting those claims, the government alleges that this case should be dismissed at the outset, pushing the common law "state secrets privilege" beyond all previous boundaries. To justify this broad expansion of executive power, the government must misstate what this case is actually about. Plaintiffs here do not seek information concerning how or why the NSA selects intelligence targets. Nor do they seek the details of how the NSA engages in its widely publicized data-mining of telephone and email records. Rather, the claims at issue here arise from a few very simple and non-classified facts.

Contrary to the government's contentions, AT&T's participation in surveillance activities is simply not a state secret. At AT&T's [redacted] Facility, for example, internet traffic arrives at the [redacted] Room through a fiber-optic cable. In that room, a copy of the internet traffic that AT&T receives – email, web browsing requests, and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service – is diverted onto a separate fiber-optic cable through the use of a "[redacted]." The cabinet in turn is then connected to equipment in a special room, called the [redacted] Room. The [redacted] room was created under the supervision of the NSA, contains powerful computer equipment capable of analyzing large volumes of data and connecting to separate networks,

distinct from the commercial AT&T network. Only personnel with NSA clearances – people assisting or acting on behalf of the NSA – have access to the [redacted] Room.

These acts constitute "interception" in violation of Title III of the Communications Act of 1934, and improper "electronic surveillance" in violation of the Foreign Intelligence Surveillance Act of 1978 ("FISA"). And when AT&T intercepted for the government Plaintiffs' and class members' communications without a warrant, it violated the Fourth Amendment of the United States Constitution. What the government did with that internet traffic after it was delivered by AT&T is not a necessary element of, or even particularly relevant to, Plaintiffs' claims.

These facts are not classified. Many of Plaintiffs' claims here are supported by evidence that has already been established to be beyond the ambit of the state secrets privilege: the testimony and documents of Mark Klein, a former AT&T technician who was not employed by the government and had no security clearance from the NSA, and the analysis of that evidence by former Senior Advisor for Internet Technology at the FCC, J. Scott Marcus. On March 30, 2006, the government was given an opportunity to review Mr. Klein's materials to evaluate whether to object to their use in this litigation. Far from invoking the state secrets privilege to cover those materials, the government instead allowed Plaintiffs to go forward. The government cannot unring that bell.

Plaintiffs have further alleged that AT&T also violated its customers' rights by turning over the customer detail records from its "Daytona" database system. When it did so, AT&T engaged in a "disclosure" also barred by, *inter alia,* the Stored Communication Act. Plaintiffs have also alleged warrantless surveillance of purely domestic telephone communications. As set forth in Section V, discovery corroborating these highly publicized events, which have not been denied by key government sources, can proceed without endangering state secrets.

Not only can Plaintiffs make their case without implicating the state secrets privilege, but AT&T can also defend itself – if it has a *bona fide* defense – without endangering state secrets. Congress has provided that if AT&T really did act with a valid government "authorization," then such an authorization cannot be cloaked as a "state secret" in order to dismiss this case. To do so

would grant AT&T a blank check to continue or even expand the illegal surveillance and render illusory the private rights of action that Congress enacted as part of FISA, rights that Congress enacted in response to perceived abuses of the use of electronic surveillance conducted for national security. Alternatively, to the degree that confidentiality might attach to some aspect of such a certification, Congress has enacted laws that render them discoverable subject to appropriate safeguards.

The government's contention that this case should be dismissed and/or summarily adjudicated on the basis of the state secrets privilege is therefore flawed for five reasons.

First, absent truly exceptional circumstances (inapplicable here), the state secrets privilege constitutes a narrow evidentiary common law privilege and not an immunity from suit. In the area of electronic surveillance Congress has specifically limited the applicability of the state secrets privilege by statute. This common law privilege cannot render the Court powerless to review the violation by a civil defendant of eavesdropping and electronic surveillance laws passed by Congress. Nor does this common law privilege shield massive violations of the Fourth Amendment by the country's largest telecommunications company from judicial scrutiny and redress. *See* Section I.

Second, a close examination of the elements of proof required by Plaintiffs' claims demonstrates that the case does not turn on state secrets. On the contrary, these claims are fully supported by the government's existing admissions, by the Klein testimony and documents, and by Plaintiffs' expert, J. Scott Marcus. The government simply cannot repossess information that is already of record and transform it into a state secret. Nor should the government be permitted to evade judicial review by inaccurately recharacterizing Plaintiffs' claims as requiring proof of state secrets. *See* Section II.

Third, the statutory scheme bars the government from contending that the state secrets privilege can prevent disclosure of any alleged certification provided to AT&T – and as a corollary proposition that this case must be dismissed. As noted, that contention effectively nullifies the private rights of action Congress created to regulate electronic surveillance.

Moreover, the government's contention regarding the secret status of the certification defense is particularly meritless given the facts of this case. The only reason that the government and AT&T have asserted to bar disclosure of the possible certifications is that the existence or non-existence of a certification would tend to prove or disprove whether AT&T was involved in the alleged surveillance activities. That argument falls flat for the simple reason that AT&T's actions in divulging its customers' communications to the NSA are already set forth in non-secret record evidence.

Fourth, given the breadth of AT&T's violations of law there is no doubt that Plaintiffs have standing to assert their claims. AT&T engaged in a wholesale disclosure of customer information. AT&T cannot now contend that no individual customer has standing because it has inflicted an injury on all of them. Nor does the state secrets privilege bar the discovery of information pertinent to standing; indeed, the core facts are already of record. *See* Section IV.

Finally, summary judgment is plainly premature. Before such a procedure would be appropriate, the government must articulate with specificity why the privilege pertains to specific categories of information. The state secrets privilege could then be applied to concrete disputes, as the law requires. In the meantime, non-privileged discovery should proceed. Beyond the record already established, Plaintiffs are empowered by express statutory provisions to take further discovery in support of their claims. *See* Section V.

The government's proposition that this Court must summarily dismiss a case that is based upon non-secret evidence alleging a broad violation of fundamental constitutional rights of millions of American citizens is extraordinary, and extraordinarily dangerous. It seeks to use a common law evidentiary privilege to eliminate private rights of action created by Congress specifically to redress improper telecommunications surveillance. And it seeks to bar judicial review of a key constitutional question – the application of the Fourth Amendment to untargeted, ongoing surveillance of the private communications of millions of non-suspect Americans.

The Executive cannot deprive the Court of the ability to enforce these rights. The state secrets privilege overwrites neither the Constitution nor the express statutory scheme created by Congress. The government's assertion that it does should be denied.

STATEMENT OF FACTS

The record assembled by Plaintiffs on their pending motion for preliminary injunction – without any formal discovery – establishes the existence of a massive surveillance campaign by AT&T of email communications crossing its network. The declarations of Mark Klein and expert J. Scott Marcus establish the following key facts.

The Creation Of The [redacted] Room

Around January 2003, AT&T built a room at its [redacted] facility in San Francisco, subject to heightened security and accessible only to those with a clearance from the NSA. Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction, Dated March 28, 2006 ("Klein Decl."), ¶ 12 and Exs. A-C. The NSA was deeply involved in this process. While Mr. Klein was working at AT&T's [redacted] office in San Francisco, an NSA agent met with and interviewed a Field Support Specialist for a "special job" at the [redacted] Facility. Klein Decl., ¶ 10. In January 2003, Mr. Klein personally observed the construction of the [redacted] Room, which was nearing completion. *Id.*, ¶¶ 11-14. At that time he learned that the field support specialist was working to install equipment in the [redacted] Room. *Id.*, ¶ 14.

NSA Control Of The [redacted] Room

In October 2003, Mr. Klein was transferred to the [redacted] Facility, where his job was to oversee the [redacted] Room as a communications technician. Klein Decl., ¶ 15. In that room, communications carried by AT&T's WorldNet Internet service are directed to or from customers. Klein Decl., ¶ 19. Although Mr. Klein had keys to every other door at the [redacted] Facility, he did not have access to the [redacted] Room. *Id.*, ¶ 17. The regular AT&T technician workforce was not allowed in the [redacted] Room, which [redacted]. *Id.*, ¶ 17.

Only AT&T employees with NSA clearances had access to the [redacted] Room. Klein Decl., ¶ 17; *see also* ¶¶ 10, 14, 16-18. Executive Order No. 12968 governs NSA clearances. *See* Declaration of Michael M. Markman, filed herewith ("Markman Decl."), Ex. 1. It discusses clearance for "employees," which it defines to include all persons, whether employed by NSA or by a third party, "who act[s] for or on behalf of an agency as determined by the appropriate agency head." Exec. Order No. 12968 § 1.1(e) (1995) (emphasis added).[1] Thus, the AT&T employees cleared by the NSA act "**on behalf of the NSA**".

The Executive Order also requires that anyone granted access to classified information must have a demonstrated "need-to-know" in order to perform a governmental function. Exec. Order No. 12968 § 1.2(a) (1995), Markman Decl., Ex. 1. Absent special circumstances, eligibility also requires a demonstrated "need for access." *Id.*, § 2.1(b)(2). The regulation defines "need for access" and "need to know" in Section 1.1:

> "Need for access" means a determination that an employee requires access to a particular level of classified information in order **to perform or assist in a lawful and authorized governmental function**.
>
> "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information **in order to perform or assist in a lawful and authorized governmental function**.

Id., §§ 1.1(g) and (h) (emphasis added). Thus, the AT&T employees with NSA clearances to function within the [redacted] Room must, as a condition of their clearance, be performing or assisting in the performance of governmental functions.

The Communications Diverted To The [redacted] Room

AT&T connected fiber-optic cables in the [redacted] Facility's [redacted] Room to a "[redacted]." The cabinet diverted or copied the content of all of the electronic

---

[1] The Executive Order provides: "(a) 'Agency' means any 'Executive agency,' as defined in 5 U.S.C. 105, the 'military departments,' as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office."

communications traversing those cables into the [redacted] Room. Klein Decl., ¶¶ 19, 25-28. The "split" circuits contain domestic and international communications in transit to and from AT&T's [redacted] with the following internet networks and internet exchange points: [redacted]. Klein Decl., ¶¶ 29-34.

Based on his experience, and on his review and analysis of the Klein declaration and its exhibits, Plaintiffs' expert concludes that "**all or substantially all**" of AT&T's [redacted] traffic in San Francisco – communications between AT&T customers and non-AT&T customers – was copied into the [redacted] Room. Declaration of J. Scott Marcus in Support of Plaintiffs' Motion for Preliminary Injunction, dated March 29, 2006 ("Marcus Decl."), ¶ 104; *see id.*, ¶ 108 ("significant traffic to and from the plaintiffs (especially those in the San Francisco Bay Area)"). He also concludes the [redacted] Room acquires a substantial amount of domestic internet traffic. *Id.*, ¶¶ 109-113.

The Capabilities Of The Equipment In The [redacted] Room

The [redacted] Room contains at least one [redacted], which is designed to analyze large volumes of communications at high speed, and can be programmed to analyze the contents and traffic patterns of communications according to user-defined rules. *Id.*, ¶¶ 75, 78-85. The room also contains a [redacted]. *Id.*, ¶ 75 & n. 29. As Mr. Marcus explains, this equipment is powerful: "the [redacted] system is well suited to process huge volumes of data, including user content, in real time. It is thus well suited to the capture and analysis of large volumes of data for purposes of surveillance." *Id.*, ¶ 83; *see id.*, ¶ 75 ("surveillance is one of the system's primary functions").

The [redacted] Backbone Network

Mr. Marcus's assessment of the surveillance capability of the [redacted] Room is also based on the presence of a second backbone network. The [redacted] Room contains computer equipment and internet routers. Klein Decl, ¶ 35 ([redacted]). It is connected to an [redacted] backbone network, separate from AT&T's Common

Backbone, apparently operating at very fast speeds. Marcus Decl., *Id.*, ¶¶ 76-77, 86-87; Klein Exh. C, pp. 6, 12, 42. Mr. Marcus explains it is highly likely that "while the [redacted] Room is connected to the [Common Backbone] (from which it receives communications), it is also connected to another network, and signals can be sent out of or into the [redacted] Room over the [redacted] backbone." *Id.*, ¶ 76; *id.* at 16 (Fig. 2).

AT&T, assisting the government, may send and receive data via the [redacted] backbone network to and from the equipment in the [redacted] Room. Marcus Decl., ¶¶ 76-77. This additional network would be unnecessary if AT&T were merely using the equipment in the [redacted] Room for ordinary business purposes, because such analytical results could, and logically would, be transmitted over the Common Backbone. *Id.*, ¶¶ 76-77, 86-89.

AT&T's Other [redacted] Rooms

The evidence indicates that AT&T implemented Surveillance Configurations in cities other than San Francisco. Klein Decl., ¶ 36 ([redacted]); Marcus Decl., ¶¶113-18. For instance, Exhibit A to the Klein Declaration refers to a site in [redacted]. *Id.*, ¶ 118. A fully deployed set of Surveillance Configurations would capture a substantial fraction – likely well over half – of AT&T's purely domestic traffic, representing substantially all of the AT&T traffic peered to and from other providers. This comprises about 10% of all purely domestic internet communications in the United States. Marcus Decl., ¶¶ 119-126.

Warrantless Surveillance By The Government Using AT&T Facilities

No one contests that, shortly after the 9/11 terrorist attacks, the President directed the NSA to conduct a covert program of warrantless surveillance of telephone and internet communications within the United States. Request for Judicial Notice, filed April 5, 2006 ("RJN") at ¶¶ 1, 2; *see also* Declaration of Cindy Cohn, filed April 5, 2006 ("Cohn Decl."), Exs. C and J. The NSA surveillance program, in which AT&T's conduct allegedly plays a part, operates without judicial authorization. RJN at ¶¶ 6-7. The only review process is authorization by an NSA "shift supervisor" to review or listen to particular individuals' communication. RJN at ¶ 9. As General Hayden, Principal Deputy Director for National Intelligence, put it, the

NSA's program "is a more ... 'aggressive' program than would be traditionally available under FISA," in part because "[t]he trigger is quicker and a bit softer than it is for a FISA warrant." RJN at ¶ 10.

Additionally, the Directors of National Intelligence and the NSA have publicly admitted that the NSA's surveillance program covers at least "one-end foreign" (and thus by implication one-end domestic) communications. Declaration of John D. Negroponte ("Negroponte Decl."), at 5; Declaration of Lieutenant General Keith B. Alexander ("Alexander Decl."), at 3. The government has never denied the existence of a broader program that intercepts or collects records regarding purely domestic communications. Plaintiffs have alleged and provided evidence of such a broader program, which has also been widely reported in the press.

Homeland Security Secretary Michael Chertoff confirmed that the government has employed "'data-mining' – collecting vast amounts of international communications data, running it through computers to spot key words and honing in on potential terrorists." Cohn Decl., Ex. G. The President similarly acknowledged the existence of the call detail collection program by saying that Congress had been briefed in response to a question about the reports that the NSA compiles data. *See* Markman Decl., Ex. 2. And Senate Majority Leader Frist acknowledged that he was briefed. Markman Decl., Ex. 3. Numerous media reports have discussed the data-mining and internet interception aspects of the surveillance. *See, e.g.,* Cohn Decl. Exs. A-F; Scarlett Decl., filed April 5, 2006, Ex. 1.

ARGUMENT

I. THE STATE SECRETS PRIVILEGE DOES NOT WARRANT DISMISSAL ABSENT EXTRAORDINARY CIRCUMSTANCES NOT PRESENT HERE

A. The State Secrets Privilege Does Not Provide The Basis For Dismissing This Case

The government urges outright dismissal of this case between private litigants at the pleadings stage based on an unconstitutional and extreme view of a narrow evidentiary privilege. Absent truly extraordinary circumstances not present here, Article III courts consider assertions of the state secrets privilege in the context of specific categories of evidence.

1. The State Secrets Privilege Does Not Confer Immunity

The common law state secrets privilege does not grant absolute immunity from suit to private litigants whenever the government asserts that prosecution of the suit will risk the disclosure of unnamed state secrets. Rather, "[t]he state secrets privilege is a common law evidentiary privilege that allows the government to deny discovery of military secrets." *Kasza v. Browner*, 133 F.3d 1159, 1165 (9th Cir. 1998) (emphasis added).[2]

Ninth Circuit precedent requires that if the Court does determine that the privilege applies to a particular piece of evidence, "[t]he plaintiff's case then goes forward based on evidence not covered by the privilege." *Id.* at 1166 (emphasis added). Only "[i]f, after further proceedings, the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence" may the Court "dismiss her claim as it would with any plaintiff who cannot prove her case." *Id.* at 1166 (emphasis added). Here, the plaintiffs can prove their *prima facie* case based on a wealth of non-privileged evidence. *See* Section II, *infra.*

Plaintiffs have found no case in which dismissal was based on the mere possibility that state secrets might be sought in discovery. The existing law is to the contrary. For example, the D.C. Circuit rejected a similar attempt by the government to divorce the state secrets privilege from specific and ripe discovery disputes. *In re United States*, 872 F.2d 472, 477-79 (D.C. 1989). There, the plaintiff claimed injuries based on FBI intelligence activities. *Id.* at 473. Without answering, and divorced from the context of any discovery request, the government moved to dismiss based on the state secrets privilege. *Id.* at 473-74. As in this case, the

---

[2] *See also United States v. Reynolds*, 345 U.S. 1, 6-7 (1953) ("[T]he privilege against revealing military secrets ... is well established in the law of evidence"); *Monarch Assur. P.L.C. v. U.S.*, 244 F.3d 1356 (Fed. Cir. 2001) (using the term "common-law state secrets privilege"); *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544, 546 (2d Cir. 1991) ("The state secrets privilege is a common law evidentiary rule"); *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989) (same); *Bosaw v. Nat'l Treasury Employees Union*, 887 F. Supp. 1199, 1213 (S.D. Ind. 1995) ("[T]he government may invoke common law privileges, such as the deliberative process, investigative files, or state secrets privileges, which enable it to protect information from discovery"); *Black v. U.S.*, 900 F. Supp. 1129, 1133 (D. Minn. 1994).

government argued that "continuation of plaintiff's action will inevitably result in disclosure of information that will compromise current foreign intelligence and counterintelligence investigative activities." *Compare id.* at 478. (emphasis added) *with* Gov't Br. at 16 ("Further litigation would inevitably risk the disclosure of state secrets").

The D.C. Circuit rejected the government's premise. The court reiterated that "[t]he state secrets privilege is a common law evidentiary rule that protects information from discovery when disclosure would be inimical to the national security." *Id.* at 474. While "[o]nce successfully invoked, the effect of the privilege is completely to remove the evidence from the case," *id.* at 476, "[d]ismissal of a suit, and the consequent denial of a forum without giving the plaintiff her day in court ... is indeed draconian." *Id.* at 477. Holding that "broad application of the privilege to all of [the government's] information, before the relevancy of that information has even been determined, was inappropriate at this early stage of the proceedings," the D.C. Circuit refused to dismiss the case. *Id.* at 478.

"[T]he court is the final arbiter of the propriety" of invoking the privilege. *In re Under Seal*, 945 F.2d 1285, 1288 (4th Cir. 1991). It is empowered to determine whether illegal *ultra vires* actions prevent the government from invoking the state secrets privilege. *Black v. United States*, 62 F.3d 1115, 1119-20 (8th Cir. 1995) (assessing whether illegal actions barred the government from invoking privilege and concluding the conduct at issue was legal). Indeed, an Executive Order expressly bars the government from designating materials as classified in order to, *inter alia*, "conceal violations of law," or to "prevent embarrassment to a person, organization, or agency." Exec. Order No. 13292 (2003) (amending Exec. Order No. 12958) (attached as Markman Decl., Ex. 7).

Now, in the face of the unanimous recognition by the courts that "[t]he state secrets privilege is a common law evidentiary privilege," *Kasza*, 133 F.3d at 1165, the government attempts to cloak it in the garb of a constitutionally enshrined Executive power.[3] *See, e.g.*, Gov't

---

[3] The government rightly conceded at oral argument that the state secrets privilege is a common law evidentiary privilege. Markman Decl., Ex. 4 at 35:3-11. While the government argued that

Mem. at 8 (citing *United States v. Nixon*, 418 U.S. 683, 710 (1974)); Gov't Br. of May 24, 2006 at 12-13. The Court in *Nixon*, however, nowhere stated that the privilege is enshrined in the Constitution. Rather, the Court merely stated that in that case, the President "d[id] not place his claim of privilege on the ground they are military or diplomatic secrets. As to these areas of Art. II duties the courts have traditionally shown the utmost deference to Presidential responsibilities." 418 U.S. at 710. In *Reynolds*, which the government also invokes, the Court pointedly refused to enshrine the privilege in the Constitution, holding only that this position "ha[d] constitutional overtones which we find it unnecessary to pass upon, there being a narrower ground for decision." 345 U.S. at 6.

This common law privilege can be preempted by Act of Congress. *See* Section I.B.1, *infra.* It does not abrogate the Court's power and responsibility to provide a forum for cases and controversies. *See Reynolds*, 418 U.S. at 709-10 ("Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers"); *In re Grand Jury Subpoena Dated Aug. 9, 2000*, 218 F. Supp. 2d 544, 560 (S.D.N.Y. 2002) ("[T]he contours of the privilege for state secrets are narrow, and have been so defined in accord with uniquely American concerns for democracy, openness, and separation of powers"). And this common law privilege does not grant private litigants broad immunity from suit at the pleadings stage merely because the government claims that unwritten discovery requests might ultimately seek state secrets.

2. The Exceptional Authority To Dismiss A Case Where Its Subject Matter Is A State Secret Does Not Exist Here

This is not a case where early dismissal is required because "the 'very subject matter of the action' is a state secret." *Kasza*, 133 F.3d at 1166 (citing *Totten*, 92 U.S. 105 (1875) (2 Otto) at 107). The courts have only imposed the draconian sanction of dismissal on the grounds of the state secrets privilege in extraordinary circumstances, when "the whole object of the suit and of the discovery is to establish a fact that is a state secret." *Molerio v. FBI*, 749 F.2d 815, 821 (D.C.

---

this privilege is "constitutionally based," *id.*, Ex. 4 at 35:24-25, it is not a Constitutional right or power. Congress can amend, clarify, or modify it by statute.

Cir. 1984) (emphasis added). Here, AT&T's participation in the government's program is already well-established by record evidence that is not a state secret: *inter alia,* the testimony and documents of Mr. Klein proving that AT&T diverted its customers' communications to a secure room to which only those with NSA security clearances had access, and the expert testimony of Mr. Marcus concluding that this operation was only consistent with surveillance activities. *See* Statement of Facts, *supra.* The central issue in this case is simply whether these actions by AT&T, Inc. and AT&T Corp. – private defendants – violated well-defined statutory and Constitutional prohibitions against intercepting and disclosing customers' communications. This is without regard to how, why, when, or where the government might use those communications (or not) in its domestic spying program. Plaintiffs' case, therefore, is unlike the small handful of cases in which a court dismissed an action at the pleading stage.

For example, in *Totten*, the plaintiff alleged that he had contracted with President Lincoln himself to engage in secret spying activities during the Civil War. 92 U.S. at 105. The only issue in the case was whether or not "a contract for secret services" existed between him and the government. *Id.* at 107. The Court dismissed the lawsuit because "the existence of a contract of that kind" – that is, a secret contract for secret services – "is itself a fact not to be disclosed." *Id.* In contrast, this is not a case requiring the establishment of a contract for secret services. The Fourth Amendment, FISA, and similar laws are not secret; Plaintiffs' claims under them require only the establishment of AT&T's interception and disclosure of its customers' communications – facts already established by the record evidence. *See* Section II, *infra*.

This case is also unlike those lower court cases in which the consideration of otherwise garden-variety privacy disputes required probing into details regarding classified government weapons systems or intelligence programs. For example, this case is unlike *Sterling v. Tenet*, 416 F.3d 338 (4th Cir. 2005), in which a CIA agent sued under Title VII, alleging racial discrimination in the form of disparate treatment. *Id.* at 341. There, the plaintiff's claims would have required him to present evidence regarding "the relative job performance of [CIA] agents, details of how such performance is measured, and the organizational structure of CIA

intelligence gathering." *Id.* at 347. Here, Plaintiffs need not inquire into the details of the government's work to prove its case against AT&T.[4]

For the same reasons, this case is wholly different from *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991). There, the estate of a sailor killed when his ship was fired on by foreign aircraft sued defense contractors for negligence, claiming that the ship's weapons systems were negligently designed, manufactured, and tested. *Id.* at 546. The court dismissed the case because the subject matter of the suit – the alleged negligent design of weapons systems – required discovery of the specifications for the weapons and defense systems aboard the ship as well as the procedures governing their use. *Id.* All of these details were state secrets. *Id.* Further, the plaintiff "ha[d] not designated any sources of reliable evidence on the factual issues going to liability." *Id.* at 548. Here, Plaintiffs need not probe into such details regarding the government's program to make its case.

Fitzgerald v. Penthouse, 776 F.2d 1236 (4th Cir. 1985), was a libel suit for damages between two private parties. One party wanted to use in the litigation classified evidence to which it had no constitutional or statutory right of access to support its claim that the statements were true, and so not libelous. *Id.* at 1238. He attempted "to call expert witnesses with knowledge of relevant military secrets" to do so. *Id.* at 1243. Since "truth or falsity of a defamatory statement is the very heart of a libel action," *id.* at 1243 n.11, state secrets were central to the case. *Id.* at 1243. Here, Plaintiffs' claims are directed at AT&T's activities, not the government's program. Moreover, unlike here, in *Fitzgerald* there was no claim challenging the constitutionality of ongoing executive action or contending that the defendant had participated in a violation of the plaintiff's constitutional or statutory rights.

Finally, this case is also unlike a recent decision from the Eastern District of Virginia, cited by the government in its response to the Court's May 17 minute order, which dismissed a

---

[4] Unlike *Sterling v. Tenet, Edmonds v. United States DOJ*, 323 F. Supp. 2d 65, 69 (D.D.C. 2004), and *Tilden v. Tenet*, 140 F. Supp. 2d 623, 626 (E D. Va. 2000), which were all claims based on employment relationships with intelligence agencies.

lawsuit brought by a German citizen against the Director of the CIA. *El-Masri v. Tenet*, 2006 WL 1391390 at *1-3 (E.D. Va. May 12, 2006). In *El Masri*, the plaintiff alleged constitutional and statutory violations following his abduction by CIA operatives in an "extraordinary rendition" program. El Masri's claims required him to establish specific treatment to which he was subjected by the CIA in the course of an alleged clandestine intelligence operation. *Id.* at 5. According to the court, the whole object of the suit was not merely to establish the existence of the rendition program but to establish "the means and methods the foreign intelligence services of this and other countries used to carry out the program," requiring dismissal. *Id.* at 5.

In contrast, Plaintiffs' claims here do not require proof of the reasons or methods of interception, or what the government did with the communications and data once AT&T provided them. Nor do Plaintiffs' claims require discovery of the criteria the government employs to select targets for further review of a communication after AT&T has unlawfully intercepted or disclosed it. The only focus of Plaintiffs' claims is on AT&T's activities – the act of intercepting and disclosing customer information to the government. And Plaintiffs will prove these key facts on the basis of non-classified information. *See* Section II.B and C, *infra*.

It bears emphasis that the Supreme Court has never used the *Totten* bar to dismiss claims alleging an ongoing violation of an individual constitutional liberty like the Fourth Amendment. The rights at issue in the *Totten* and *Tenet* cases were rights that arose from an employment relationship created between the plaintiff and the executive, not substantive restrictions on executive action contained in the Constitution.[5] *Tenet* repeatedly makes clear the *Totten* rule is limited to claims arising out of a secret espionage relationship: "the longstanding rule, announced more than a century ago in *Totten*, prohibiting suits against the Government based on covert espionage agreements," *id.* at 3; "*Totten* precludes judicial review in cases such as

---

[5] Although the *Tenet* plaintiffs raised due process claims as well, these claims were entirely derivative of the alleged employment agreement and would not exist if there was no agreement, as the Supreme Court recognized. *Tenet*, 544 U.S. at 8. Plaintiffs' Fourth Amendment rights at issue here, by contrast, are substantive rights created by the Constitution, and do not arise out of an agreement with the government.

respondents' where success depends upon the existence of their secret espionage relationship with the Government," *id.* at 8; "*Totten's* broader holding that lawsuits premised on alleged espionage agreements are altogether forbidden," *id.* at 9; "*Totten's* core concern [is] . . . preventing the existence of the plaintiff's relationship with the Government from being revealed." *Id.* at 10.[6]

B. Congress Has Limited The State Secrets Privilege In The Context Of Electronic Surveillance

The government skirts two foundational truths: that the Constitution gives Congress the power to delimit the scope of the state secrets privilege, and that Congress has in fact exercised that power in the area of telecommunications surveillance through the FISA statute. In particular, Congress has crafted private rights of action to prevent unlawful electronic surveillance, as well as specific statutory provisions addressing how purported state secret information should be handled so as not to extinguish those explicit rights.

1. Congress Has The Power To Limit The Government's Ability To Invoke The State Secrets Privilege

While the government suggests that Congress cannot limit the common law state secrets privilege without violating the separation of powers, Gov't May 24, 2006 Br. at 13, that is manifestly not the case. *See Tenet v. Doe*, 544 U.S. 1, 11 (2005) (Stevens, J., concurring) ("Congress can modify the federal common-law rule announced in *Totten*"). In the *Kasza* decision, relied upon for much of the government's argument, the Ninth Circuit considered whether the Resource Conservation and Recovery Act of 1976 (RCRA), 42 U.S.C. § 6001, preempts the common law state secrets privilege. *Kasza*, 133 F.3d at 1167. Far from determining that Congress cannot limit the state secrets privilege, the Court engaged in a searching analysis of the statutory scheme of the RCRA to assess its implications for the state

---

[6] Similarly, as noted above, the lower court cases the government relies on did not concern constitutional challenges.

secrets privilege. Ultimately, the Court held that the environmental statute did not speak to the common law state secrets privilege.

Ignoring authority that includes Congress' War Powers under Article 1, Section 8 of the Constitution, the government envisions a regime of executive power in which Congress ostensibly has no role in legislating in areas of national security. The authorities cited by the government are inapposite. Both *Dep't of the Navy v. Egan*, 484 U.S. 518 (1988), and *Dorfmont v. Brown*, 913 F.2d 1399 (9th Cir. 1990), discuss the discretion to approve security clearances, which is not governed by statute (and is not solely within the authority of the executive). *See Egan*, 484 U.S. at 530 (basing its holding on the absence of a pertinent statute: "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs"). Neither case considered the statutes at issue here – 50 U.S.C. §§ 1806(f), 1825(g), 1845(f), or 18 U.S.C. § 2511(2)(a)(ii)(B). As explained below, these Acts of Congress speak directly to, and curtail, the applicability of the state secrets privilege.

2. Congress Has Directly Spoken To The Application Of The State Secrets Privilege In Electronic Surveillance Cases

In the area of electronic surveillance, Congress has narrowed the common law state secrets privilege by a statute that "speaks directly to the question otherwise answered by federal common law." *Kasza*, 133 F.3d at 1167 (quoting *County of Oneida v. Oneida Indian Nation*, 470 U.S. 226, 236-37 (1985) (quoting *City of Milwaukee v. Ill.*, 451 U.S. 304, 315 (1981))) (quotation marks and brackets omitted). In particular, Congress created FISA as the "exclusive means by which electronic surveillance ... may be conducted." 18 U.S.C. 2511(2)(f) (emphasis added).

In the context of FISA and other statutes, Congress created private rights of action against telephone companies (and others) conducting illegal electronic surveillance, directing the Court to use a particular procedure to carefully determine the applicability of the state secrets privilege, and empowering the Court to take appropriate "safeguards" to protect national security

during the Court's oversight of the adversary process. The government's view of the state secrets privilege amounts to a *de facto* elimination of those statutory rights.

a. Congress created private rights of action to enforce strict rules governing electronic surveillance

Under FISA, a federal officer acting on behalf of the President, through the Attorney General, may obtain a court order "approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information." 50 U.S.C. § 1802(b). In adopting FISA, Congress provided:

> the procedures in this chapter or chapter 121 or 206 of this title [18 USCS §§ 2510 et seq., or 2701 et seq., or 3121 et seq.] and the Foreign Intelligence Surveillance Act of 1978 [50 USCS §§ 1801 et seq.] shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act [50 USCS § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

18 U.S.C. § 2511(2)(f) (emphasis added). Otherwise stated, Congress adopted FISA "to curb the practice by which the executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 8, 1978 U.S.C.C.A.N. at 3910.

As part of this statutory regime, Congress has unquestionably created rights and authorized the United States District Courts to try them. Congress specifically created several private rights of action for illegal electronic surveillance:

- "An aggrieved person, other than a foreign power or an agent of a foreign power ... who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 [50 USCS § 1809] of this title shall have a cause of action against any person who committed such violation...." 50 U.S.C. § 1810.

- "Except as provided in section 2511(2)(a)(ii) [18 USCS § 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." 18 U.S.C. § 2520(a) (Section 2511(2)(a)(ii) allows the disclosure of information in response to court order or FISA certification).

- "Except as provided in section 2703(e) [18 USCS § 2703(e)], any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter [18 USCS §§ 2701 et seq.] in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind 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." 18 U.S.C. § 2707(a) (Section 2703(e) allows the disclosure of information in response to a warrant or governmental subpoena).

- "Any person aggrieved by any [unauthorized publication or use of communications] may bring a civil action in a United States district court or in any other court of competent jurisdiction." 47 U.S.C. § 605(e)(3)(A).

Congress knew when it adopted these private causes of action that, by their very nature, the trial of cases involving secret electronic surveillance will involve matters within the scope of the common law state secrets privilege. Nevertheless, Congress created them – demonstrating that Congress intended the Courts to hear such cases. As the Second Circuit observed in a state secrets case against the government involving a patent with military application that was withheld under a secrecy order:

> Unless Congress has created rights which are completely illusory, existing only at the mercy of government officials, the act [providing a private cause of action] must be viewed as waiving the privilege. Of course, any such waiver is dependent upon the availability and adequacy of other methods of protecting the overriding interest of national security during the course of a trial.

Halpern v. U.S., 258 F.2d 36, 43 (2d Cir. 1958) (emphasis added).

Congress adopted FISA one hundred and three years after the Supreme Court first recognized the state secrets privilege in *Totten*, 92 U.S. at 107, and twenty-four years after the *Reynolds* decision relied on by the government. *See* FISA, P.L. 95-511, Title I, § 106, 92 Stat. 1793 (Oct. 25, 1978). It cannot be said to have been unaware of the state secrets privilege when creating these private rights. By the same token, the government cannot use the common law state secrets privilege to squelch Congressionally mandated rights regarding violations of the electronic surveillance statutes.

b. Congress provided for disclosure of the existence of electronic surveillance through "legal process"

Section 2511(2)(a)(ii) directly addresses disclosures regarding the existence of electronic surveillance or the devices used in such activity. The provision requires:

> No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, ***except as may otherwise be required by legal process*** and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate.

18 U.S.C. § 2511(2)(a)(ii) (emphasis added).

In this subsection, Congress signaled that information regarding the existence of surveillance, and the means used to implement it, should be confidential. Congress, however, also recognized that such disclosures could be required by "legal process".

The government and AT&T contend that the term "legal process" empowers the Executive to invoke the state secrets privilege to prevent any disclosure. But that interpretation of "legal process" is so broad it eviscerates the disclosure that Section 2511(2)(a)(ii) authorizes. Gov't May 24, 2006 Br. at 17 n.10; AT&T May 24, 2006 Br. at 17-18. Rather, the statute's reference to disclosure subject to "legal process" effectuates the Congressional purpose of establishing private causes of action to enforce FISA rights. Without that provision, the unchecked proclivity of the executive to bar all information regarding the invasion of such rights could render such a private claim a nullity. *See Reiter v. Sonotone Corp.*, 442 U.S. 330, 339 (1979) ("[I]n construing a statute we are obliged to give effect, if possible, to every word Congress used"). Whatever disclosure subject to "legal process" may mean, it cannot mean that, on the whim of an official (even a high placed one), there be no disclosure and therefore no rights of action.

The more logical and Constitutionally consistent construction derives from reading this provision against the backdrop of ordinary discovery procedures, subject to safeguards available to the Court in the form of protective orders providing for limited access to sensitive information.

That interpretation balances the two concerns that Congress was directly addressing in the statute: the need to make sure that security was protected, and the need to make sure that the rights created by FISA were not eliminated though excessive deference to the executive.

c. Congress provided for discovery of classified materials pertinent to the legality of the surveillance in 50 U.S.C. §§ 1806(f) and 1845(f)

Congress has also enacted provisions governing disclosures where the state secrets privilege is applicable and even where the government believes the disclosure would harm national security. 50 U.S.C.§ 1806(f). The law provides:

> Whenever any motion or request is made by an aggrieved person ... to discover or obtain applications or orders or other materials relating to electronic surveillance ... the United States district court ... shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Id. (emphasis added).

Through this provision, Congress enacted a FISA discovery procedure that is to be followed "notwithstanding any other law" – which necessarily includes the common law state secrets privilege. The Conference Report for FISA noted that "the conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests." H.R. Conf. Rep. No. 95-1720, 1978 U.S.C.C.A.N. 4048, 4061 (Oct. 5, 1978); *see also* S. Rep. No. 95-701, 1978 U.S.C.C.A.N. 3973, 4032-33 (Mar. 14, 1978) (calling Section 1806(f) "a reasonable balance between an entirely in camera proceeding ... and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.").

Further demonstrating its intent, Congress passed two laws adding provisions parallel to Section 1806(f) governing the use of pen registers and trap-and-trace devices, Intelligence Authorization Act for 1999, Pub. L. 95-511, Title IV, § 405, as added Pub. L. 105-272, Title VI, § 601(2), 112 Stat. 2408 (Oct. 20, 1998) (codified at 50 U.S.C. § 1845(f)), and physical searches. Intelligence Authorization Act For Fiscal Year 1995, Pub. L. 95-511, Title III, § 305, as added Pub. L. 103-359, Title VIII, § 807(a)(3), 108 Stat. 3449; (Oct. 26, 2001) (codified at 50 U.S.C. § 1825(g)). These provisions demonstrate Congress' specific intent that the government not be permitted merely to declare surveillance to be a "state secret" and thereby eliminate the possibility of judicial review.

As recently as October 2001, Congress reaffirmed its decision to provide for discovery regarding electronic surveillance notwithstanding the state secrets privilege. Even after the September 11 attacks, Congress maintained a private right of action against the United States for violations of one of the same electronic surveillance statutes under which Plaintiffs have sued AT&T here. *See* 18 U.S.C. § 2712(a). As part of the congressionally mandated process for litigating such claims against the United States, Congress directed, "[n]otwithstanding any other provision of law," that the procedures set forth in Section 1806(f), 1825(g), and 1845(f) are the "exclusive means by which certain materials may be reviewed." 18 U.S.C. § 2712(b)(4).

Where the alleged secret in some way implicates the legality of the surveillance, the Court is empowered to direct disclosure of the classified material – subject to appropriate safeguards. Any other result would indeed render the statute's private rights of action "completely illusory, existing only at the mercy of government officials." *Halpern,* 258 F.2d at 43. FISA reduced any Presidential authority in this area to its "lowest ebb." H.R. Conf. Rep. 95-1720 (1978) at 35, reprinted in 1978 U.S.C.C.A.N. 4048, 4064 (quoting *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579, 635 (1952) (Jackson, J., concurring)).

d. The government cannot manufacture immunity from the statutory disclosure requirements by disregarding FISA altogether

In the face of FISA's unambiguous language, the government and AT&T assert – without the support of statutory text or any interpretative authority – that Section 1806(f) cannot apply unless the government has used FISA to authorize the electronic surveillance. June 6, 2006 Order at 6:15-21 (quoting Gov't May 24, 2006 Br. at 11; AT&T May 24, 2006 Br. at 10). Otherwise stated, they argue that electronic surveillance conducted outside FISA is not subject to Section 1806(f). But the government's (and AT&T's) argument runs afoul of the express statutory language that FISA constitutes the "exclusive means by which electronic surveillance ... may be conducted." The government and AT&T did not have the choice simply to ignore FISA and the legal safeguards established by Congress, nor are actions taken in violation of FISA to be treated as "outside the statute."[7]

The plain language demonstrates that the discovery authorized by Section 1806(f) applies beyond FISA surveillance. Specifically, Section 1806(f) broadly applies "whenever any motion or request is made … [1] to discover or obtain applications or orders or other materials relating to electronic surveillance or [2] to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act...." 50 U.S.C.§ 1806(f)(emphasis added). The limitation "under this Act" only applies to the last antecedent "electronic surveillance." *See Anhydrides & Chemicals, Inc. v. United States*, 130 F.3d 1481, 1483 (Fed. Cir. 1997) ("Referential and qualifying words and phrases, where no contrary intention appears, refer solely to the last antecedent, which consists of the last word, phrase, or clause that can be made an antecedent without impairing the meaning of the sentence"). Thus, Congress adopted two clauses, one for "electronic surveillance" and the other for "electronic surveillance under this Act." This plain language interpretation is consistent with the reason Congress enacted Section

---

[7] The government also has taken the position that Plaintiffs must first prove that they are "aggrieved persons" before they can have access to the secret materials under Section 1806(f). Gov't May 24, 2006 Br. at 11. Plaintiffs have done so, as discussed in Section II.B.

1806(f) – to permit the courts to assess the legality of particular electronic surveillance – an important component of which is whether the surveillance complies with FISA. Section 1806(f) applies to electronic surveillance, whether that surveillance satisfies FISA or not.

AT&T also incorrectly implies that FISA does not apply in civil cases. *See* AT&T May 24, 2006 Br. at 10. This contradicts the language of the statute and Congress' express purpose in adopting it. One of the three events that can trigger a disclosure is a civil motion to compel – demonstrating that Section 1806(f) is not limited to warrants against individuals under FISA. 18 U.S.C. § 1806(f). The legislative history confirms that Section 1806(f) applies with equal force in civil proceedings: "The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases." H.R. Conf. Rep. No. 95-1720, 1978 U.S.C.C.A.N. 4048, 4061 (Oct. 5, 1978).

AT&T further contends that "the great weight of authority interpreting the FISA sections plaintiffs cite mandates that 'even ordinary FISA surveillance information over which no formal state secrets claim has been asserted' should not be disclosed." AT&T May 24, 2006 Br. at 11. The cited cases, however, do not hold that disclosure to the aggrieved party is inappropriate, as AT&T implies. In *United States v. Belfield*, 692 F.2d 141 (D.C. Cir. 1982), for example, the court merely rejected the argument "that in every case 'such disclosure is necessary to make an accurate determination of the legality of the surveillance.'" *Id.* at 147 (emphasis added). AT&T's cases all recognize that courts do have the power to disclose the information to the aggrieved person. *See, e.g., ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 462 (D.C. Cir. 1991). Those courts held merely that the particular facts of each individual case supported the conclusion that disclosure to the aggrieved person was not necessary.

3. Congress' General Directives To The NSA Do Not Change The Procedure For Discovery Regarding Electronic Surveillance

The government cites two general statutory provisions that provide for the authority of the NSA and the Director of National Intelligence, but do not address the specific electronic surveillance issues at issue here. *See* Gov't May 24, 2006 Br. at 12 n.6. Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402, note, and Section 102A(i)(1) of the

Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), unremarkably provide for the protection of our country's national secrets. These two general statutes do not conflict with Sections 1806(f) and similar statutes. Section 6 protects the organization, function, and activities of the NSA – but it only protects those that are secret. For example, the NSA has a website (www.nsa.gov) that has extensive explanations of the NSA's organization, function, and activities. The NSA could not reasonably claim that this public information falls under Section 6.

In the same vein, Plaintiffs do not seek to discover secret information about the NSA or its activities. As discussed below, they intend to use information in the public domain and information that Congress has made discoverable under Sections 1806(f), 1845(f), and 2511(2)(a)(ii)(B). While the general statutes cited by the government require that the DNI "protect intelligence sources and methods from unauthorized disclosure," 50 U.S.C.§ 403-1(i)(1) (emphasis added), disclosure pursuant to Sections 1806(f), 1845(f), and 2511(2)(a)(ii)(B) are not only authorized but required by Congress.

Even if the general statutory provisions somehow did conflict with Section 1806(f), the latter must prevail. Two principles of statutory construction require this result. First, Section 1806(f) is a specific provision, and in a conflict with more general statutes the specific statute governs. *See Edmond v. U.S.*, 520 U.S. 651, 657 (1997). Second, "a specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it has not been expressly amended." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000). "This is particularly so where the scope of the earlier statute is broad but the subsequent statutes more specifically address the topic at hand...." *Id.* (quoting *United States v. Estate of Romani*, 523 U.S. 517, 530-31 (1998)).

As shown above, Section 1806(f) specifically applies to the subject of this case: electronic surveillance. The statutes cited by the government do not. Both Section 6 and Section 102A(i)(1) merely discuss the general protection of the "information and activities" of the NSA and "intelligence sources and methods." None of the cases cited by the government find

otherwise. They merely prevent the use of the Freedom of Information Act to access various types of sensitive national security information and have no bearing on the electronic surveillance at issue here.

C. The State Secrets Privilege Cannot Permit Dismissal Of Claims Seeking Relief From Ongoing Violations of Constitutional Rights

The judicial authority to consider claims arising under the Constitution further limits the state secrets privilege, rendering dismissal improper. No branch of government can waive or refuse to obey the limitations on government power set forth in the Fourth Amendment – or prevent another branch from enforcing those limitations. The Fourth Amendment depends entirely on the judiciary for its enforcement. "The effect of the Fourth Amendment is to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority, and to forever secure the people, their persons, houses, papers and effects against all unreasonable searches and seizures under the guise of law." *Elkins v. United States*, 364 U.S. 206, 209 (1960). It has been established from the earliest days that the judiciary, as a coequal branch, has and must have the power to pass upon the legality of executive action, and the duty to do so when the issue is presented to it in a case or controversy. *Marbury v. Madison*, 5 U.S. 137, 177 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is"). The executive is without authority to restrict the scope of the judicial power of this Court to consider the application of the Fourth Amendment.

The Supreme Court recently reaffirmed the continuing vitality of the judiciary as a co-equal branch of government which must stand ready to adjudicate individual rights notwithstanding assertions regarding national security. In *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), the habeas petitioner Hamdi was a citizen captured with enemy forces on a foreign field of battle and held as an "enemy combatant" without trial or charges in executive detention in the United States. The executive asserted that the Article III court could not exercise its habeas jurisdiction to adjudicate the factual basis of Hamdi's detention, *i.e.*, whether he was in fact an enemy combatant. The executive contended this fact was nonjusticiable and was exclusively within the power of the executive to determine, just as the executive claims here

that Plaintiffs' constitutional challenge to the alleged massive, warrantless executive searches and seizures is nonjusticiable.

In *Hamdi*, the Court rejected the notion that the executive's national security powers can restrict the scope of constitutional liberties or negate the power of the judiciary to adjudicate claims by citizens for invasions of those liberties. The four-justice plurality held that "we necessarily reject the Government's assertion that separation of powers principles mandate a heavily circumscribed role for the courts in such circumstances." *Hamdi*, 542 U.S. at 535. It noted that the claim of executive supremacy, no different than the one made by the government here:

> cannot be mandated by any reasonable view of separation of powers, as this approach serves only to condense power into a single branch of government. We have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens. *Youngstown Sheet & Tube*, 343 U.S., at 587. 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.

Hamdi, 542 U.S. at 535-36 (plur. opn.) (first emphasis original, second emphasis added); *accord*, *Webster v. Doe*, 486 U.S. 592, 603 (1988) (a "'serious constitutional question' ... would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim"). Four other Justices were even more emphatic in their rejection of the executive's assertion that the courts were powerless to adjudicate the factual basis of Hamdi's constitutionally-created habeas corpus claim. *Hamdi*, 542 U.S. at 553 (conc. opn. of Souter, J.), 576 (dis. opn. of Scalia, J.).

"[I]t would turn our system of checks and balances on its head to suggest that a citizen could not make his way to court with a challenge to the factual basis for his detention by his government, simply because the Executive opposes making available such a challenge." *Hamdi*, 542 U.S. at 536-37. So too here, it would turn our constitutional system on its head to hold that Plaintiffs were barred from offering proof that AT&T is violating the Fourth Amendment by its program of warrantless, suspicionless mass searches and seizures under color of law, and barred

from seeking relief for those violations "simply because the Executive opposes making available such a challenge."[8]

II. PLAINTIFFS' CLAIMS CANNOT BE DISMISSED ON THE GROUNDS OF THE STATE SECRETS PRIVILEGE BECAUSE THEY ARE BASED ON NON-SECRET INFORMATION

A. The State Secrets Privilege Does Not Change the Standard of Review

The government's reliance on the state secrets privilege does not change the standard of review for determining whether to dismiss this case pursuant to Rule 12, or whether to grant summary judgment. Should the state secrets privilege apply to exclude evidence in this case, "[t]he plaintiff's case then goes forward based on evidence not covered by the privilege." *Kasza*, 133 F.3d at 1166. "[I]nvocation of the privilege results in no alteration of pertinent substantive or procedural rules…." *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983); *see Molerio v. FBI*, 749 F.2d 815, 822 (D.C. Cir. 1984) (applying Rule 56 standard to decide summary judgment in state secrets case); *Black v. U.S.*, 900 F. Supp. 1129, 1135 (D. Minn. 1994) (same).

Accordingly, the Court should not grant the government's motion to dismiss "unless it appears beyond doubt that the plaintiff can prove no set of facts in support of the claim that would entitle it to relief." *Williamson v. Gen. Dynamics Corp.,* 208 F.3d 1144, 1149 (9th Cir. 2000). Plaintiffs' "allegations of material fact are taken as true and construed in the light most favorable to the nonmoving party." *Burgert v. Lokelani Bernice Pauahi Bishop Trust,* 200 F.3d 661, 663 (9th Cir.2000). "Summary judgment is to be granted only where the evidence is such that no reasonable jury could return a verdict for the non-moving party." *Black*, 900 F. Supp. at

---

[8] The Supreme Court recently reiterated that litigation is strongly protected against government interference, not only on First Amendment grounds but also to protect the integrity of judicial review. *See generally Legal Services Corp. v. Velazquez*, 531 U.S. 533, 542, 545-550 (2001) (holding publicly funded legal services attorneys' representation of indigent clients was "private speech"). Courts depend on attorneys' freedom to speak in litigation "for the proper exercise of the judicial power." *Id.* at 545-46. The government is "seeking to prohibit the analysis of certain legal issues and to truncate presentation to the courts," which is "inconsistent with the proposition that attorneys should present all the reasonable and well-grounded arguments necessary for proper resolution of the case." *Id.* at 545. The courts "must be vigilant" when the government seeks in effect to insulate its own conduct "from legitimate judicial challenge." *Id.* at 548.

1135 (citing *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 250 (1986)). "In determining whether summary judgment is appropriate, the evidence offered by the non-moving party is to be believed and all justifiable inferences therefrom are to be drawn in a light most favorable to that party." *Black*, 900 F. Supp. at 1135 (citations omitted).

B. The Government Cannot Retroactively Transform Non-Secret Information Into A State Secret

The state secrets privilege does not bar from the courtroom information that already is in the public domain. *See Spock v. U.S.*, 464 F. Supp. 510, 518 (S.D.N.Y. 1978). In *Spock*, the plaintiff sued the government for unlawful interception of his oral, wire, telephone, and telegraph communications. *Id.* at 512. Just as it does here, the government in *Spock* argued that the case had to be dismissed because "defendants can neither admit nor deny the allegations of the complaint without disclosing state secrets." *Id.* at 519. The plaintiffs countered that "[t]his one factual admission or denial ... reveals no important state secret, particularly since the interception of Dr. Spock's communications was previously disclosed in an article in the *Washington Post*, dated October 13, 1975." *Id.* The court agreed with plaintiffs and declined to dismiss the case:

> [h]ere, where the only disclosure in issue is the admission or denial of the allegation that interception of communications occurred, an allegation which has already received widespread publicity, the abrogation of the plaintiff's right of access to the courts would undermine our country's historic commitment to the rule of law.

Id. at 520; *see also Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1306 (1983) (noting Court has not "permitted restrictions on the publication of information that would have been available to any member of the public"); *McGehee v. Casey*, 718 F.2d 1137, 1141 (D.C. Cir. 1983) (noting "[t]he government has no legitimate interest in censoring unclassified materials" or "information ... derive[d] from public sources").

The principle that the government cannot engage in after-the-fact reclassification of non-secret information as "state secrets" applies with even greater force in this case. Here, the key facts have not only been the subject of widespread publicity, but they are based on (1) the government's own statements, (2) the Klein testimony and documents from Mr. Klein that are of

record in this case, and (3) the expert testimony of Mr. Marcus, analyzing the evidence provided by Mr. Klein.

The state secrets privilege cannot strike from the record *ex post* the evidence already adduced by Plaintiffs in the form of the Klein Declaration and supporting exhibits (the "Klein Evidence"), or of the expert opinion of Mr. Marcus analyzing that evidence.[9] Mr. Klein came into possession of the Klein Evidence first-hand. He has never been an NSA employee. He did not become privy to this evidence as a result of any agreement with the government, or by virtue of any security clearance. The information learned first-hand by Mr. Klein – a private citizen with no government association – cannot possibly be "secret" in any relevant sense. *Cf. NSN Int'l Indus. v. E.I. Dupont de Nemours & Co.*, 140 F.R.D. 275 (S.D.N.Y. 1991) (holding state secrets privilege not waived where attorneys for defendant government contractor received security clearances before reviewing classified documents).[10]

Finally, it does not follow from the government's asserted inability to "confirm or deny" the facts set forth in the Klein Evidence that this case must be dismissed. The government can take any view it chooses of the substance of the Klein Evidence – that is its prerogative. What the government cannot do is remove that evidence from the record and seek to have this case adjudicated as if it did not exist.

---

[9] The specific manner in which the Klein Evidence establishes contents of the Klein Evidence establish Plaintiffs' *prima facie* case is discussed in Section II.B, *infra*.

[10] Even if the government could have invoked the state secrets privilege to prevent Plaintiffs from submitting the Klein Evidence to the Court, it affirmatively chose not to do so. Plaintiffs discussed the Klein Evidence with the Justice Department on March 30, 2006. Declaration of Lee Tien re Partial Filing of Documents in Support of Motion for Preliminary Injunction ("Tien PI Decl."), ¶¶ 9-12. At the Justice Department's request, Plaintiffs hand-delivered it copies of the Klein Evidence. *Id.,* ¶¶ 13-14. By letter of April 4, 2006, the Justice Department informed Plaintiffs that the government did not object to the filing of the Klein Evidence under the Court's normal sealing procedures. Declaration of Lee Tien in Support of Admin. Mots. to Extend Page Limit for Mot. for Preliminary Inj., ¶ 5; *id.,* Ex. A (April 4, 2006 Letter of Mr. Anthony J. Coppolino, Special Litigation Counsel, DOJ).

C. Plaintiffs' Prima Facie Case Is Established Based On The Klein Evidence, Expert Analysis, and Government Admissions – It Does Not Require State Secrets

Plaintiffs' statutory claims can be grouped into two categories: (1) claims turning on AT&T's unlawful "interception" of either the contents of communications or non-content information relating to communications, and (2) claims turning on the "divulgence" or "disclosure" of the contents of communications or other customer information. The requirements of both sets of claims are satisfied by Plaintiffs' evidence.

1. Plaintiffs' Interception Claims

Plaintiffs allege two statutory claims based principally on AT&T's acts of unlawful interception of either (i) the contents of communications, or (ii) non-content information relating to communications: Counts III and II of the Amended Complaint.[11]

a. Count III – Violation of 18 USC § 2511

Count III is based on AT&T's intentional interception of wire and electronic communications, barred by Title III, 18 U.S.C. § 2511(1)(a). The statute defines "intercept" as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). "Contents" include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8).

The Klein Declaration and its exhibits show that AT&T designed, installed, and implemented a system that copies massive quantities of electronic communications traversing its network, and shunted them into a secure room. Access to that room was restricted to AT&T employees cleared by the NSA. *See* Statement of Facts, *supra,* at 5-7.

When AT&T copies the communications into the Surveillance Configuration described in the Klein and Marcus declarations, those communications have been "intercepted" within the

---

[11] Plaintiffs discuss Count III (interception of electronic communications) before Count II (electronic surveillance) as first in logical order.

meaning of the statute. *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992) (holding in context of telephone communications that "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time").[12] Internet traffic constitutes a "communication" within the meaning of the statute. *Id.* ("The phrase 'or other' was inserted into ... Title III to ensure privacy protection for new forms of communication such as electronic pagers, electronic mail, and computer-to-computer communications."); *see also Konop,* 302 F.3d at 878 (for transmission of website); *United States v. Councilman*, 418 F.3d 67, 79-80 (1st Cir. 2005) (for email).

b. Count II – Violation of 50 U.S.C. §§ 1809-10

Count II is based on AT&T's electronic surveillance, in violation of FISA, 50 U.S.C. §§ 1809-10. See 50 U.S.C. §§ 1809, 1810. FISA creates a private right of action against a person who:

> (1) engages in electronic surveillance under color of law except as authorized by statute; or
>
> (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

50 U.S.C. § 1809 (establishing criminal liability); 1810 (creating private right of action).[13]

---

[12] *See In re State Police Litigation,* 888 F. Supp. 1235 (D. Conn. 1995). There, the court found the interception of telephone communications despite the government's argument they listened to recorded tapes "only to the extent necessary." The court noted that "a telephone conversation that is recorded, but not necessarily listened to, is still an 'interception' under the Act." *Id.* It explained, "[t]he terms of the statute itself support plaintiffs' interpretation. If Congress had intended the phrase 'aural or other acquisition' to mean 'overheard,' it certainly could have employed the simpler term. The section's additional requirement that a conversation be acquired 'through the use of any electronic, mechanical, or other device' suggests that it is the act of diverting, and not the act of listening, that constitutes an 'interception.' * * * [W]hile the Act does not precisely define what an interception is, it must be deemed to have occurred 'when the contents of wire communications are captured or redirected in any way'" *Id.* (decision also gathers cases).

[13] Section 1810 specifically provides that "[a]n aggrieved person" (defined in § 1801(k) as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance") "other than a foreign power or an agent of a foreign power … who has been subjected to an electronic surveillance or about whom

These provisions of FISA apply to AT&T's conduct here. *First,* "electronic surveillance" includes the acquisition in the United States by surveillance device of the contents of wire communications to or from a person in the United States under circumstances where a warrant would be required for law enforcement purposes. 50 U.S.C. § 1801(f)(2). *Second,* "contents, when used with respect to a communication," include "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n) (emphasis added). *Finally,* a "wire communication" is "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l).[14]

The Klein Evidence, and the expert analysis of Mr. Marcus, establishes that AT&T has created a copy of the internet traffic that it handles. Not only did the "the traffic that was diverted represent[] all, or substantially all, of AT&T's [redacted] traffic in the San Francisco Bay Area", but the "traffic intercepted at the [redacted] facility probably represented a substantial fraction of AT&T's total national [redacted] traffic." Marcus Decl., ¶¶ 104, 107 (emphasis added). This traffic included purely domestic-to-domestic communications (*id.*, ¶¶ 109-112), was diverted wholesale by AT&T's [redacted] into the room controlled by the NSA (*id.*, ¶¶ 46, 49, 104-112) – and was accessible only to those performing or assisting in a governmental function (thereby acting under color of law). *See* Exec. Order No. 12968, §§ 1.1(g), (h), 1.2(a) (1995) (attached as Markman Decl., Ex. 1).[15] For its part, the government has admitted that it has not

---

information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation …." 50 U.S.C. § 1810.

[14] Under Title III, "wire communications" relate to "aural transfers" – telephone calls – while under FISA "wire communications" can include data.

[15] Any further doubts as to the fact of government involvement will be resolved when AT&T produces any government-issued certifications, which as explained below, are not protected by the state secrets privilege.

obtained a warrant authorizing this acquisition. *See* RJN at ¶¶ 6-7, 9. By any measure, this was an "acquisition" of the "contents" of a "wire communication" under the prohibitions of U.S.C. § 1809(a)(1).

By the same token, under 50 U.S.C. § 1806(f) and similar statutes (*see* Section I.B.2 *supra*), Plaintiffs are entitled to take discovery regarding AT&T's disclosure to the NSA of call detail records and the contents of telephone call. The mere fact of an enormous interception of the contents of telephone communications violates FISA, the SCA, and Section 2511 – regardless of whether or not the government chooses only to listen to targeted telephone calls (a question that is immaterial to Plaintiffs' claims).

2. Plaintiffs' "Divulgence/Disclosure Claims"

Plaintiffs' second set of claims is based on the divulgence, disclosure, or use of communications contents or other information. Each of these is described below.

a. Count III – 18 U.S.C. §§ 2511(1)(c), (d), and (3)(a)

Section 2511 goes beyond the act of "interception," discussed above in Section II.B.1.a. It also prohibits a range of conduct that includes divulgence and disclosure of electronic communications. The evidence supports Plaintiffs' Count III on these independent bases for liability without regard to anything that would be privileged as a "state secret."

First, Section 2511(1)(c) prohibits any person from "intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." In other words, if AT&T knew or should have known that it had intercepted any domestic-to-domestic email or telephone call, and then intentionally disclosed that communication to the government, then AT&T faces liability.

Second, Section 2511(1)(d) prohibits any person from "intentionally us[ing], or endeavor[ing] to use, the contents of any … electronic communication" knowing that the information was intercepted in violation of the statute. As noted above, AT&T must have known

that it had intercepted vast numbers of communications. Klein Decl., ¶¶ 19, 25-34; Marcus Decl., ¶¶ 46, 49, 104-112. Whether or not the government reviewed the communication is legally irrelevant under Section 2511(1)(c) and (d) – what matters for assessing liability under Section 2511(1)(c) is AT&T's act of intentional disclosure, and under (1)(d) is AT&T's act of intentional use.

Third, Section 2511(3)(a) imposes special obligations on an "electronic communication service" like AT&T. When operating an electronic communications service, these entities must not "intentionally divulge the contents of any communication ... while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."[16]

The evidence reveals that all three happened here. First, AT&T must have known it had intercepted the communications – that was the very purpose of the [redacted] that it instructed Mr. Klein to install. Klein Decl., ¶¶ 19, 25-29. And that cable unquestionably carried domestic-to-domestic communications. *Id.*, ¶¶ 29-31, 34. Second, the intentional act of shunting these communications off, on a separate cable (*id.*, ¶ 27), into a room controlled by the NSA (*id.*, ¶ 17) that included sophisticated data-mining software and hardware (*id.*, ¶ 35), was an actionable disclosure under Section 2511(1)(c). Third, AT&T gave the government the means to review the communications, resulting in a "use" under Section 2511(d) and in the "divulging" of the communications under Section 2511(3)(a). Indeed, the Klein and Marcus declarations show that

---

[16] Plaintiffs' claim for violation of 47 U.S.C. § 605 (Count IV) is an independent but substantially similar basis for liability. Section 605 prohibits "any person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio" from "divulg[ing] or publish[ing] the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception," to anyone not authorized to see it. AT&T unquestionably transmits and assists in the transmission of "communications by wire." Klein Decl., ¶¶ 19, 25-29, 34. The record evidence also unquestionably shows that, at a minimum, AT&T divulged the existence of the emails received on its fiber-optic cable to the government via the [redacted] and cable into the [redacted] Room. *Id.*, ¶ 34. The President himself conceded at a press conference that the NSA program collects "lists" of communications, and the Director of Homeland Security has spoken to the issue of data-mining from large quantities of data about communications. Statement of Facts, *supra,* at 9.

the [redacted] Room contains sophisticated equipment such as the [redacted], which can analyze large amounts of communications traffic in real time. Klein Decl. ¶ 35; Marcus Decl. ¶¶ 78-90. On these facts, it is highly likely that the communications contents entering the [redacted] Room are being subjected to sophisticated computer analysis, and are thus being "used."

In addition, AT&T is known to maintain massive databases of call detail records (CDR) data. As an anonymous government source discussed with *USA Today*, AT&T disclosed this data to the government. Markman Decl., Exh. 5. Congress has empowered Plaintiffs, as aggrieved parties whose telephone communications and call data records were disclosed to the government, to take discovery about AT&T's surveillance. *See* Section I.B.2, *supra.*

b. Counts V and VI – The Stored Communications Act (18 U.S.C. § 2702(A))

Title 18 U.S.C. § 2702 sets out rules of conduct for "electronic communications services" and for "remote computer services." The basis for Count V – Section 2702(A)(1) – requires that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

Similarly, the basis for Count VI – Section 2702(A)(3) – requires that "a provider of … electronic communications 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." 18 U.S.C. § 2702(A)(3). Sections 2702(A)(1) and (A)(3) compliment one another. While (A)(3) protects data relating to a customer and his or her communications, but not the content of the communications themselves, Section (A)(1) protects stored contents.

Again, the Klein and Marcus declarations, and government admissions, support liability under both prongs of this statutory regime. This evidence not only shows that AT&T "[redacted]" fiber-optic circuits so that the communications on those circuits were copied into the [redacted] Configuration, and that access to the [redacted] Room was controlled by the NSA, but also that AT&T

had furnished the room with sophisticated storage hardware. Klein Decl., ¶ 35. This indicates that at least for some period of time electronic communications data was stored in the room. What is more, the [redacted] Configuration was itself connected to a separate and distinct network called the [redacted] Backbone. *Id.* On these facts, it is highly likely that communications entering the [redacted] Room were being stored by AT&T for the NSA. Indeed, based on Executive Order 12968, the [redacted] Room itself, furnished by AT&T, is controlled by those acting on behalf of, or to assist, the NSA. This evidence thus establishes the predicate facts of a violation of Section 2702(A)(1). The government's admissions establish violation of Section 2702(A)(3) – this includes the gathering of "lists of calls" and of data-mining (Statement of Facts, *supra,* at 9). Any remaining doubts as to the factual basis for Plaintiffs' disclosure claims can be resolved by targeted discovery to determine whether the [redacted] Backbone is for AT&T's sole use, or whether it is being used to send any communications (whether the content of communications or non-content data) to another person. For purposes of these claims, it is irrelevant whether that other person is the government.[17]

AT&T's disclosure of call data records, as reported by *USA Today*, is also a violation of the Stored Communications Act because AT&T stores that data in an enormous database, nick-named "Daytona," before disclosure to the government. As discussed above, Congress declared such action illegal, and has given Plaintiffs the power to take discovery to enforce their rights.

In sum, a wealth of non-privileged evidence supports Plaintiffs' claims. Plaintiffs are also entitled to take discovery concerning the legality of the surveillance at issue, and are empowered to take discovery of other non-privileged matters as well. Dismissal is unwarranted.

D. The Constitutional Claims

Almost 40 years ago, the Supreme Court held that the Fourth Amendment applies with full force to prevent the government from indiscriminate surveillance of private communications. *Katz v. U.S.*, 389 U.S. 347, 352 (1967); *Berger v. N.Y.*, 388 U.S. 41, 58-59 (1967). Indeed,

---

[17] The only exception is 18 U.S.C. § 2702(a)(3) (Count VI).

"[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." *Id.* at 63. The threat is to speech as well as privacy, causing First Amendment harm. *United States v. U.S. Dist. Ct. (Plamondon)*, 407 U.S. 297, 314 (1972) ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power.").[18] Because of the "grave constitutional questions" posed by electronic communications surveillance, courts bear "a heavier responsibility" in supervising the fairness of such procedures. *Osborn v. U.S.*, 385 U.S. 323, 329 n.7 (1966).

The warrant requirement of the Fourth Amendment unquestionably applies to electronic surveillance of purely domestic electronic communications. *Plamondon*, 407 U.S. at 321-22 (1972). Here there is no dispute that the government has proceeded in the absence of a warrant. The evidence already in the record supports the conclusion that domestic-to-domestic transmissions were intercepted by AT&T and provided to the government. The question of "state action" also does not turn on information that might fall within the ambit of the "state secrets" privilege. The state secrets privilege creates no impediment to Plaintiffs' Fourth Amendment claim.

1. The Constitution Requires That The Government Obtain A Warrant Based On A Particularized Showing Of Probable Cause

The Fourth Amendment requires that the government or its agents act pursuant to a warrant based on probable cause before engaging in electronic surveillance. *Plamondon*, 407 U.S. at 316; *Keith*, 407 U.S. at 321-322 (holding warrant requirement applies with equal force to domestic national security surveillance); *Berger*, 388 U.S. at 59 (holding probable cause requirement intended "to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed."). The need for particularity, which the warrant requirement addresses, " is especially great in the case of eavesdropping"

---

[18] Such fear currently deters plaintiff Jewel's speech and associational activity. Jewel Decl., ¶8 (refraining from Internet research on certain topics and curtailing association with Muslim correspondent in Indonesia).

because of the inevitable interception of intimate communications unrelated to the legitimate investigation. *Berger*, 388 U.S. at 56; *cf. Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding Fourth Amendment requirements must be applied with "scrupulous exactitude" where First Amendment rights implicated).

The wholesale surveillance alleged here complies with none of the core warrant requirements, and is unconstitutional on these grounds alone. It constitutes an unlawful seizure under the Fourth Amendment. *Berger,* 388 U.S. at 41. As the Supreme Court found in *Berger,* "a roving commission to 'seize' any and all conversations" is unconstitutional. *Id.* (holding unconstitutional the monitoring of conversations of "any and all persons coming into the area covered by" surveillance device would "be seized indiscriminately and without regard to their connection with the crime under investigation"). AT&T's decision to disclose the contents of its "Daytona" database – the call data records of millions of customers – is equally indiscriminate and unlawful. Nor can the mass surveillance alleged here, which reveals the contents of private communications, internet activities, and the associational relationships of millions of Americans, possibly be "narrowly tailored" to achieving any compelling government interest. *Ashcroft v. ACLU*, 542 U.S. 656, 666 (2004). It therefore also violates the First Amendment.

The question of "reasonableness," which the government suggests must be answered under *Halkin II*, is of no moment. The warrantless surveillance at issue in *Halkin II* – where all that was known about the government's surveillance was that they had created watchlists of individuals associated with Vietnam War protest groups – is not remotely comparable to this case. 690 F.2d at 1000. This case involves the interception and disclosure of truly massive volumes of communications and data about those communications. Klein Decl. ¶¶ 34-35. This includes "all or substantially all" of the AT&T [redacted] email traffic for the entire San Francisco Bay Area. Marcus Decl., ¶ 104. While the government may be compiling watchlists based on those millions of communications and that mountain of data, such watchlists are not the basis for Plaintiffs' claims. Plaintiffs' claims are based on the indiscriminate interception and disclosure of those communications and that data by AT&T.

2. No Exception To The Warrant Requirement Exists In This Case

The government incorrectly argues that the purported foreign surveillance and special needs exceptions to the warrant requirement bar Plaintiffs' Fourth Amendment claims here. Plaintiffs allege that AT&T has captured purely domestic-to-domestic communications and data for the government, and members of foreign governments (and terrorist groups like al Qaeda) are excluded from Plaintiffs' class.

a. The purported "foreign surveillance" exception, which has not been recognized by the Supreme Court, is inapplicable

The Supreme Court has never held that the President may authorize warrantless surveillance for national security purposes or otherwise. Indeed, the Court rejected that argument in the context of domestic surveillance for purposes of national security. *Plamondon*, 407 U.S. at 321 ("A prior warrant establishes presumptive validity of the surveillance …. By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur"). The Supreme Court's reasoning applies to surveillance within the United States for purposes of foreign intelligence. *Id.* at 320-21 (noting risks to "privacy of speech" from unregulated surveillance, judicial competence to review "difficult issues," and minimal disclosure risks in *ex parte* warrant proceeding).

This case is also far outside the foreign surveillance powers of the executive for at least two additional reasons. First, Plaintiffs allege, and the evidence shows, that AT&T is acquiring electronic communications indiscriminately. *See* Statement of Facts, *supra,* at 6-7. Even were it the government's intent to actually listen in only on communications of the suspected agents of foreign powers, the totally indiscriminate nature of the seizure by AT&T on behalf of the government bars any "foreign surveillance" exception. *See Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986) (Scalia, Circuit J. for the court) ("It is now clear that [the warrant] requirement attaches to national security wiretaps that are not directed against foreign powers or suspected agents of foreign powers").

Second, a "foreign surveillance exception to the Fourth Amendment" warrant requirement, were it recognized by the Supreme Court, would have to be narrowly drawn in light of FISA's statement of Congressional intent. In FISA, Congress has directly and specifically spoken on the question of domestic warrantless wiretapping, including during wartime. Congress comprehensively regulated all electronic surveillance in the United States, authorizing such surveillance only pursuant to specific statutes designated as the "exclusive means by which electronic surveillance ... and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

When Congress enacted this language, it repealed an earlier Title III provision providing that "[n]othing contained in this chapter or in section 605 of the Communications Act of 1934 shall limit the constitutional power of the President ... to obtain foreign intelligence information deemed essential to the security of the United States." 18 U.S.C. § 2511(3) (1976).[19] Congress properly concluded that:

> the basis for this legislation is the understanding -- concurred in by the attorney general -- that even if the president has an "inherent" constitutional power to authorize warrantless surveillance for foreign intelligence purposes, congress [h]as the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.

S. Rep. No. 95-604(I), at 16, 1978 U.S.C.C.A.N. at 3917.

Congress exercised its power with the intent to control executive power to employ electronic surveillance. The basis for this legislation is the understanding – shared by the Attorney General – that even if the President has an "inherent" constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance. *Id.*; *see also id.* at 4, 1978 U.S.C.C.A.N. at 3905-06 (Attorney General Bell's testimony regarding Administration's position); S. Rep. No. 95-701, at 6-7, 1978 U.S.C.C.A.N. at 3975.

---

[19] FISA § 201(c), 92 Stat. 1797.

The need to comply with FISA for the collection of foreign intelligence information through electronic surveillance is reiterated in Executive Order No. 12333 ("United States Intelligence Activities" (December 4, 1981), as amended), Section 2.5, dealing with Attorney General approval required for certain collection techniques:

> 2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken **unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.**

Exec. Order No. 12333 § 2.5 (1981) (emphasis added) (attached as Markman Decl., Ex. 8).

The decision of the FISA court in *In re Sealed Case*, 310 F.3d 717, 742 (U.S. F.I.S. Ct. Rev. 2002), an *ex parte* proceeding, is not to the contrary. Where Congress has exercised its constitutional authority and thereby has withdrawn electronic surveillance, as defined by FISA, from the "zone of twilight" between Executive and Legislative constitutional authorities, the President's asserted inherent authority to engage in warrantless electronic surveillance is thereby limited. The *In re Sealed Case* court did not address this important issue.

b. The "special needs" exception is inapplicable

Nor are AT&T's alleged actions excused by the "special needs" doctrine, which permits "minimal intrusions" on privacy rights, sometimes including warrantless, suspicionless searches when the existence of "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring); *see also Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (finding that "minimal intrusions" may be allowed in certain circumstances). This case is not one involving a high-speed police chase, border checkpoints,[20] sobriety checkpoints,[21] or drug

---

[20] *U.S. v. Martinez-Fuerte*, 428 U.S. 543 (1976).

testing programs.[22] Indeed, no court has applied the "special needs" exception to permit suspicionless wiretapping or communications surveillance of any kind, much less the indiscriminate, mass surveillance alleged and described here. *See Edmond*, 531 U.S. at 44 ("We cannot sanction stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime"). The ongoing interception and divulgence of millions of private communications over the course of years cannot reasonably be described as a minimal intrusion.

In essence, the government argues that the legality of AT&T's surveillance cannot be evaluated under our most fundamental Fourth Amendment principles because facts about "special needs" – the government's justification – cannot be revealed. The government's assertion would insulate from judicial review every possible mass surveillance program so long as the government can allege a fact-based defense like "special needs." Were this Court to accept the government's position "at this high level of generality," in spite of the record evidence demonstrating indiscriminate, mass electronic surveillance, "the Fourth Amendment would do little to prevent such intrusions from becoming a routine part of American life." *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000); *id.* at 56 (Thomas, J., dissenting) ("I rather doubt that the Framers of the Fourth Amendment would have considered 'reasonable' a program of indiscriminate stops of individuals not suspected of wrongdoing"). The Court's choice is simple: turn electronic surveillance into a Fourth Amendment-free zone, or hold that the Constitution imposes a meaningful burden of accountability upon the government.

---

[21] *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990).

[22] *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989) (government employees); *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602 (1989) (railway workers after train accidents); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995) (student-athletes); *Bd. of Educ. v. Earls*, 536 U.S. 822 (2002) (high school students).

3. Proving AT&T's Violation Of The Fourth Amendment Does Not Require Probing State Secrets

a. The evidence establishes a violation of the warrant requirement

As explained above, Plaintiffs have already alleged and introduced evidence that amply establishes a *per se* Fourth Amendment violation. The Klein Evidence and Marcus' expert analysis establish that AT&T has engaged in wholesale, suspicionless surveillance of millions of private communications. The government's public statements establish that this was perpetuated without a warrant. RJN, ¶¶ 6-7. Indeed, no court could ever issue a constitutionally valid warrant for this kind of surveillance, because it is a "general search" forbidden by the Fourth Amendment. *See* Section II.D.1, *supra.* Particular intelligence gathering methods, the names of individual targets, or the content of intercepted communications are all unnecessary to plaintiffs' case.

b. AT&T's actions as an agent of the government are not protected by the state secrets privilege

To be liable for violations of the Fourth Amendment AT&T must have been acting as an instrument or agent of the government in effecting this surveillance. *United States v. Walther*, 652 F.2d 788, 792 (9th Cir.1981) (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971)). The two critical factors in determining whether the defendants were acting as the "instrument[s] or agent[s]" of the government are: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends. *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982). Both the Klein Evidence and the purported certifications establish these points – and both are outside the state secrets privilege.

The Klein Evidence establishes that the government knew of and acquiesced in AT&T's design and implementation of the [redacted] Room to capture myriad private communications traversing their backbone network. An NSA agent personally interviewed and cleared one of AT&T's technicians to install equipment in the [redacted] Room, and ordinary AT&T technicians were not permitted there. See Klein Decl., ¶ 17. The available facts further indicate

not only that the government is highly likely to have access to the communications captured by the [redacted] Room, but that it is highly unlikely that AT&T had any independent reason to design and construct the room. *See* Marcus Decl. ¶¶ 128-139.

Separate from the Klein Evidence, any certifications that AT&T may have obtained will indicate its role as an agent of the state. As noted in Section III, below, such certifications cannot constitute a "state secret" given the statutory scheme enacted by Congress. Any evidence related to AT&T's purported certification will establish the presence of "state action" without the need for secret evidence.

III. THE ALLEGED SECRET CERTIFICATION DEFENSE DOES NOT PROVIDE THE BASIS FOR DISMISSING THIS CASE

The government argues that even if Plaintiffs can make out their affirmative case, AT&T may have received a certification from the government that would constitute a statutory defense.[23] Title III provides that the government may authorize a communication service provider or other person to assist in communications interception under Title III or electronic surveillance under FISA. 18 U.S.C. § 2511(2)(a)(ii).

The government further asserts that "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," and is therefore within the state secrets privilege. Gov't May 24, 2006 Br. at 24. The government contends that dismissal (or summary judgment) in AT&T's favor is appropriate because the state secrets privilege "deprives the defendant of information that would otherwise give the defendant a valid defense to the claim." Gov't Mem. at 15.

This position must be rejected for three reasons. First, to prohibit disclosure of the

---

[23] The governmental admissions to date show that there has been no signed court order satisfying 18 U.S.C. § 2511(2)(a)(ii)(A). *See* RJN at 6-7, 9. The only question, therefore, is whether there has been extra-judicial authorization that satisfies § 2511(2)(a)(ii)(B). Such a certification is only available in four specific instances, and the procedures of Title III and FISA are the "exclusive means" by which interceptions and electronic surveillance may be conducted. *See* Opposition to AT&T Corporation's Motion to Dismiss, filed June 6, 2006, at 15-17.

certification provided by FISA to constitute the basis for dismissal would effectively repeal the private rights of action provided by that very statute. Second, Congress has by statute expressly provided for disclosure of evidence of such certifications pursuant to ordinary "legal process." Third, the government's contention that the existence of the certifications must remain a secret because they might confirm or deny AT&T's participation in surveillance carries no weight in a case where the record evidence already establishes that AT&T actually did participate, and the protection is sought to hide ongoing and broad constitutional violations.

A. "Secret Certifications" Would Eliminate The Private Rights Of Action Created By Congress

Congress created enforceable private rights of action when it enacted FISAand a mechanism to allow an aggrieved party to gather evidence to support a claim. *See* Section I.B.2.a, *supra*. Congress specifically allowed "legal process" as a basis to disclose the existence of the interception or surveillance or the device used to accomplish the interception or surveillance. 18 U.S.C. § 2511(2)(a)(ii). The certification provision thereby creates a possible defense to the private rights created by the other provisions of that same statute, and provides a mechanism by which the defense can be raised (or lost), pursuant to "legal process." While the parties disagree about the scope of the "legal process" disclosure provision (*see* Section I.B.2.b, *supra*), one point is indisputable: the statute could not decree that the certifications themselves were a "state secret" without thereby eliminating both the private rights of action created by FISA and the possible defense that a certification provides.

The government's argument demonstrates this point all too clearly. According to the government, the fact that the certifications are an alleged "secret" means that the case cannot go forward without violating AT&T's due process rights. Gov't May 24, 2006 Br. at 17; Gov't Mem. at 21-23; AT&T May 24, 2006 Br. at 15-19. Thus, **if** the statute contemplated that the certifications were themselves a secret, then all causes of action brought under FISA would need to be dismissed at the threshold. Congress would have nonsensically created "illusory" causes of action. *Halpern,* 258 F.2d at 44.

B. Title 18 U.S.C. § 2511(2)(a)(ii) Provides For Disclosure Of Certifications Where The Underlying Surveillance Has Been Established Using Non-Classified Evidence

Whether AT&T acted illegally cannot be a secret. The government cannot use the state secrets privilege to hide illegal activities. *See*Section I.A.1, *supra* (citing *Black*, 62 F.3d at 1119-20; Exec. Order No. 13292 (2003) (amending Exec. Order No. 12958)). Markman Decl., Ex. 7. Rather than providing for "secret certifications," the provisions in 18 U.S.C. § 2511(2)(a)(ii) require quite the opposite – disclosure of the surveillance itself subject to "legal process". If the surveillance is subject to disclosure, then the certification that authorized it cannot be a secret.

This point is underscored by the briefs filed by the government and by AT&T on May 24, 2006. There, the government and AT&T identified only one reason why the certifications could be classified as a secret: to protect the confidentiality of AT&T's participation in the surveillance program. *See* Gov't May 24, 2006 Br. at 17; AT&T May 24, 2006 Br. at 15-19; *see also* Gov't Mem. at 21-23. Because that very fact – the existence of the surveillance program and AT&T's participation – is subject to the disclosure provisions of Section 2511(2)(a)(ii), the contention that the certifications themselves must be kept secret falls of its own weight.

To the degree that "legal process" contemplated by the statute is qualified by a concern over protecting confidential government information, the phrase is best understood in light of 50 U.S.C. § 1806(f). As noted above, that provision balances the government's interest in maintaining confidentiality with the private rights of action created by statute by giving the Court discretion to disclose the allegedly confidential information regarding the surveillance to the "aggrieved person" subject to appropriate safeguards. *See* Section I.B.2, *supra*.

Where the information at issue is not the surveillance itself but merely the certification authorizing the surveillance, such "safeguards" need not be so stringent as to exclude counsel for a party, and access should be granted liberally. Indeed, where the existence of the surveillance program has been established through non-classified information, the statutory scheme provides no reason to maintain the secrecy of the alleged certifications.

Finally, the government and AT&T advance the Catch-22-inspired notion that if there is no proof of an order or certification, then Section 2511(2)(a)(ii)(B) does not apply and therefore its disclosure provision is inapplicable. Gov't May 24, 2006 Br. at 17; Gov't Mem. at 21-23; AT&T May 24, 2006 Br. at 15-19. That puts matters backwards. The statute requires that AT&T have a certification before permitting electronic surveillance. Without it, AT&T would be in violation of the law. If AT&T wants to accept the benefits of a certification defense then it must accept the disclosure requirements that are written into the statutory provision that creates that defense.

C. The Certifications Cannot Be Classified As A "Secret" For Purpose Of Maintaining the Secrecy Of AT&T's Surveillance Activities When Such Activities Are Already Established By Record Evidence

While the government argues that the existence or non-existence of a certification would tend to prove or disprove whether AT&T was involved in the alleged surveillance activities, whatever force that argument might have in some other context collapses here in light of the fact that AT&T's disclosure of its customers communications to the NSA are already set forth in non-secret record evidence. The Klein and Marcus evidence fully establishes the fact of AT&T's participation surveillance on behalf of the NSA. It is one thing for the government to bootstrap "state protection" for certifications on the theory that it is necessary to protect intelligence activity that might be a secret. It is quite another for the government to attempt such a bootstrapping maneuver where the underlying activity has already been established on the basis of non-secret evidence.

IV. STANDING CAN BE ESTABLISHED WITHOUT IMPLICATING FACTS PROTECTED BY THE STATE SECRETS PRIVILEGE

The government also seeks dismissal on the grounds that Plaintiffs cannot establish standing without seeking discovery that will run afoul of the state secrets privilege. As set forth in Plaintiffs' Opposition to AT&T Corporation's Motion to Dismiss (at 4-7), facts sufficient to establish standing have been adequately pleaded. The government's additional contention that the state secrets privilege precludes Plaintiffs from establishing standing rests on a misapprehension of Plaintiffs' claims. Plaintiffs' standing relies, like the rest of their case, on

non-privileged evidence. Plaintiffs' standing is based on what AT&T did with Plaintiffs' electronic communications and data about those communications – not on what the government did with it.

A. State Secrets Are Not Necessary To Establish Plaintiffs' Injury In Fact

As explained in further detail in Plaintiffs' Opposition to AT&T Corporation's Motion to Dismiss, Plaintiffs' burden to establish standing need only be proven "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Thus, "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Id.* (quoting *Lujan*, 497 U.S. at 889). As noted in Section II above, Plaintiffs allegations concerning their actual injury rests on AT&T's non-classified conduct.

The four named plaintiffs have standing in part because all have used AT&T's services. First Amended Complaint, ¶¶ 13-16. Two of them – Carolyn Jewel and Erik Knutzen, were AT&T WorldNet subscribers and users. *Id.* Jewel remains one to this day. As alleged in the First Amended Complaint, as a result of being AT&T WorldNet subscribers and users they were subject to the invasion of their privacy rights through AT&T's disclosure of their communications. First Am. Compl. ¶¶ 13-16 and 48-64.

To the degree that a look at the record evidence is appropriate at this early stage, the non-privileged record establishes standing, at a minimum, because all or substantially all of the electronic communications sent and received by Carolyn Jewel (who resides in the San Francisco Bay Area in Petaluma, California) were intercepted and disclosed by AT&T. Specifically, Mr. Marcus' non-privileged expert testimony, based on a probing analysis of Mark Klein's testimony and the documents he provided to Plaintiffs, explains that "the traffic that was diverted represented all, or substantially all, of AT&T's [redacted] traffic in the San Francisco Bay Area." Marcus Decl., ¶ 104 (emphasis added); Klein Decl., ¶¶ 29-34.

Further, a "substantial fraction" of electronic transmissions sent and received by Erik

Knutzen, of Los Angeles, California, were also intercepted and disclosed while he was a WorldNet subscriber. Plaintiffs' expert testified that "[t]he traffic intercepted at the [redacted] facility probably represented a substantial fraction of AT&T's total national [redacted] traffic ...." *Id.*, ¶ 107. Not only that, but Mr. Marcus also offered his opinion that the evidence "*implies that a substantial fraction, probably well over half, of AT&T's purely domestic traffic was diverted, representing all or substantially all of the AT&T traffic handed off to other providers.*" *Id.*, ¶ 124 (emphasis in original). Based on his analysis of the Klein testimony and documents, Mr. Marcus also offered his opinion that one could infer "either that: (1) all of the networks with which AT&T [redacted] in San Francisco had their traffic intercepted, or else (2) any AT&T [redacted] partners whose traffic was not intercepted most likely were small networks that exchanged very little traffic with AT&T." *Id.*, ¶ 106. Indeed, Plaintiffs' expert concludes that "half of all internet traffic was likely intercepted (at least, at a physical level) for *all* AT&T customers. Moreover, it means that about 10% of all U.S. internet traffic was physically intercepted for *all* U.S. internet users, including non-AT&T customers. *Id.*, ¶ 126. The evidence reveals no effort by AT&T to filter out purely domestic-to-domestic electronic communications. Marcus Decl., ¶¶ 109-112. "A fiber [redacted], in its nature, is not a selective device – all the traffic on the [redacted] circuit was diverted or copied. *Id.*, ¶ 109.

Proof of AT&T's interception of electronic communications alone would be sufficient to establish standing. *See Berger v. New York*, 388 U.S. 41, 51, 59 (1967) (finding "the statute's failure to describe with particularity the conversations sought gives the officer a roving commission to 'seize' any and all conversations" and holding capturing a conversation sent over a telephone line is a Fourth Amendment search). Notably, Plaintiffs need not allege that AT&T has actually redirected copies of their electronic communications into the [redacted] Room. Plaintiffs need only allege that AT&T has increased the risk of such interception by installing the room. *Ecological Rights Foundation v. Pacific Lumber Co.*, 230 F.3d 1141, 1151 (9th Cir. 2000) ("An increased risk of harm can itself be injury in fact sufficient for standing."); *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000)

("Threats or increased risk thus constitutes cognizable harm"). On the evidence established to date alone, Plaintiffs have, if nothing else, established the strong likelihood that their communications were intercepted, enough to easily survive the motion to dismiss standard and enable discovery.

B. State Secrets Are Not Necessary To Establish Causation

This evidence also establishes the "causation" prong of the standing inquiry. On Plaintiffs' allegations and evidence, AT&T is acting as an agent or instrumentality of the government, and AT&T's actions have caused them injury. *Lujan*, 504 U.S. at 561-562 (explaining challenges to government action when the plaintiff is an object of the action rarely pose causation questions). The [redacted] Room is only accessible by those with an NSA clearance. Klein Decl., ¶¶ 14, 16-18. Indeed, a leak in a "large industrial air conditioner in the [redacted] Room" that "was leaking water through the floor and onto [redacted]'s equipment downstairs" could not be repaired for some days because no one with an NSA clearance was available to fix it. *Id.*, ¶ 18. By Executive Order, an NSA clearance is only available to those who are performing or assisting in a "lawful and authorized governmental function." Exec. Order No. 12968, §§ 1.1(g) and (h) (1995), Markman Decl., Ex. 1.

Finally, the government argues that Plaintiffs cannot demonstrate "prudential standing." Gov't Mem. at 17. Prudential standing exists when the injury asserted by a plaintiff arguably falls within the zone of interests to be protected or regulated by the statute in question. *FEC v. Akins*, 524 U.S. 11, 20 (1998). Title III and FISA were clearly intended to protect against unlawful surveillance, and Congress specifically provided in Title III and FISA that an aggrieved person may bring a civil action for violations of these statutes. 18 U.S.C. § 2520; 50 U.S.C. § 1810; *cf. Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997) (holding explicit grant of authority to bring suit "eliminates any prudential standing limitations and significantly lessens the risk of unwanted conflict with the Legislative Branch"). The factual predicates for establishing those

statutory violations are discussed in detail in Section II.B above.[24]

C. Plaintiffs May Take Discovery To Further Establish Standing

Were it necessary, Plaintiffs could develop further non-secret evidence through discovery from AT&T to show additional facts to demonstrate standing. *Lujan*, 504 U.S. at 561. As noted in Section V, below, discovery of non-privileged materials will further support Plaintiffs' standing. Plaintiffs submit that it will reveal the interception and disclosure of domestic telephone communications, and of call data collected by AT&T in its "Daytona" database – which will necessarily include data regarding all calls made by Plaintiffs – and provided in total to the government. These are questions that AT&T can answer with no danger to national security. *See* Section V, *infra.*

V. SUMMARY JUDGMENT IS PREMATURE ON THIS RECORD

A. The State Secrets Privilege Applies Only To Concrete Evidentiary Disputes And Should Not Be Applied Prematurely

The government's invocation of the state secrets privilege is premature because it is entirely divorced from the discovery context. Plaintiffs have sought no discovery from the government. Plaintiffs have propounded a Rule 30(b)(6) request to AT&T, regarding the existence of a certification to which no privilege can attach. *See* Section I.B.2.b, *supra*. The government thus raises this evidentiary privilege in the abstract, before any individualized discovery dispute has ripened. The vast weight of authority reveals that the privilege is applied in the context of specific discovery disputes, and not in the abstract.[25]

---

[24] The Art. III concern for "generalized grievances" also poses no barrier to plaintiffs' standing. *See* Gov't Mem. at 17. That harm is widely shared is irrelevant to Art. III. The harm should not be abstract. *Akins*, 524 U.S. at 24 (using example of large numbers of individuals injured by a widespread mass tort). The interception of all or substantially all of a customer's domestic emails, telephone calls, and call data records – along with those of potentially hundreds of thousands of other customers – is far from abstract.

[25] *See, e.g., Northrop Corp. v. McDonnel Douglas Corp.*, 751 F.2d 395, 396 (D.C. Cir. 1984) (privilege invoked in response to a subpoena *duces tecum*); *Linder v. Nat'l Security Agency*, 94 F.3d 693, 694 (D.C. Cir. 1996); *Molerio*, 749 F.2d at 819 (privilege invoked in response to motion to compel after "Defendants answered the complaint, and complied with discovery requests, although redacting many of the documents produced"); *In re Under Seal*, 945 F.2d

Mere assertions by the government or AT&T that AT&T may have a valid defense are insufficient to require dismissal. If AT&T at any point in this litigation has a defense that it believes implicates state secrets, it should be presented to the Court for review, one category of discovery at a time. The Court should decide initially whether the defense truly does implicate state secrets, and, if so, whether the defense is valid and meritorious. Only then would it even be appropriate to consider whether any of Plaintiffs' claims must be dismissed because the evidence at issue is absolutely vital to its survival. *See In re United States*, 872 F.2d at 476. Such is not (and Plaintiffs' submit never will be) the case here.

Tellingly, the government's cases did not involve dismissal at the pleadings stage. For example, the government relies on *Kasza* for the proposition that "if plaintiff cannot make out a *prima facie* case in support of its claims about the excluded state secrets, the case must be dismissed." Gov't Br. at 15. In *Kasza*, however, the Ninth Circuit held that this determination is made not at the pleadings stage, but after "further proceedings." 133 F.3d at 1166. There, the privilege was invoked only "[o]nce discovery got underway," and the government refused to provide evidence specifically "with respect to the disclosure of certain categories of national security information associated with the operating location near Groom Lake, specifically including 'security sensitive environmental data.'" *Id.* at 1163. The framing of the dispute in that specific context was crucial, because "whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter." *Id.* at 1166 (quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983)). Such is not the case here,

---

1285 (4th Cir. 1991) (privilege invoked "[a]fter several depositions and other preliminary matters were conducted," in response to a "motion to compel answers to questions that had been asked but unanswered during the deposition proceedings"); *DTM Research L.L.C. v. A.T. & T. Corp.*, 245 F.3d 327, 330 (4th Cir. 2001) (privilege invoked in response to particular discovery requests); *Bowles v. U.S.*, 950 F.2d 154, 156 (4th Cir. 1991) (privilege invoked in response to plaintiffs' discovery requests); *Heine v. Raus*, 399 F.2d 785, 787 (4th Cir. 1968) (privilege invoked during discovery); *Tilden v. Tenet*, 140 F.Supp.2d 623, 625 (E.D. Va. 2000) (privilege invoked after "Plaintiff's counsel made several discovery requests on the CIA for the production of documents and files").

where Plaintiffs have sought no discovery from the government and have thus far sought only a single category of non-privileged information from AT&T.

The government's reliance on the *Halkin* decisions (*Halkin v. Helms*, 598 F.2d 1 (D.C. Cir. 1978) ("*Halkin I*"), and 690 F.2d 977 (D.C. Cir. 1982) ("*Halkin II*"), and on *Fitzgerald*, 776 F.2d at 1241-42, are equally misplaced. Neither involved a motion to dismiss at the pleading stage. *Halkin* involved extensive discovery. The court remanded the case for further proceedings to determine if plaintiffs could prosecute some of their claims without resort to the suppressed evidence. *Halkin I*, 598 F.2d at 11. And in *Fitzgerald*, 776 F.2d at 1241-42, the government intervened to assert the privilege only on the eve of trial in specific response to the plaintiff calling witnesses to testify whether a weapons system was classified. *Id.* at 1237-38.

The government also relies on *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), as a case counseling dismissal. But in *Ellsberg*, the case was not dismissed at the pleadings stage either. Rather, the plaintiffs submitted interrogatories to the government defendants, asking for "detailed information" regarding the wiretaps at issue. *Id.* at 54. Even then, the state secrets privilege was no blunt hammer used to deprive the plaintiffs of a judicial forum. Rather, the government "admitted to two wiretaps," and selectively asserted the privilege only in response to certain other discovery requests. *Id.* The court scrutinized the application of the privilege to specific evidence, and held that only partial dismissal was necessary. *Id.* at 236.

Finally, the Court may consider careful and creative solutions to manage discovery. *See Halpern v. U.S.*, 258 F.2d 36, 43 (2nd Cir. 1958); *Loral Corp. v. McDonnell Douglas Corp.*, 558 F.2d 1130 (2nd Cir. 1977); *Spock v. U.S.*, 464 F. Supp. 510, 520 (S.D.N.Y. 1978). The Court may exercise discretion in tailoring the application of the privilege, if it applies at all, to address national security concerns without denying Article III review of the statutory and Constitutional transgressions of a public telephone company.

B. The Government Must Provide A Reasonable Explanation For The Specific Basis Of Its Assertion Of The State Secrets Privilege On The Public Record Before Summary Judgment Could Be Appropriate

The government has given the Court no basis to determine if and how the state secrets privilege ought to be applied to the facts of this case, and given Plaintiffs no basis on which to truly evaluate that contention. The state secrets privilege will only apply to shield information from discovery once the government "publicly explain[s] in detail the kinds of injury to national security it seeks to avoid and the reason those harms would result from revelation of the requested information." *Ellsberg,* 709 F.2d. at 63. If the government cannot reveal even this much information, it must then "indicate why such an explanation would itself endanger national security." *Id*. at 63-64. If the government makes an inadequate showing on the public record, its claim for privilege should be denied. *Kinoy v. Mitchell*, 67 F.R.D. 1, 9-10 (S.D.N.Y. 1975) (rejecting government's claim of privilege as to warrantless wiretapping of domestic communications due to "insufficiently specific" public declarations).

The government has met neither requirement here, discussing in its publicly filed, redacted brief and affidavits statements so general and vague that they might relate to any assertion of the state secrets privilege. Rather, the government merely repeats its conclusion – that some information ought to be privileged.[26]

As this Court noted in its Order of June 6, 2006 in deciding to review the government's *in camera, ex parte* submissions, "the Court may later require the government to provide a more specific public explanation why the state secrets privilege must be invoked". June 6, 2006 Order at 3:24-26. The government should do so now. In *Kasza,* 133 F.3d at 1182, the government provided a detailed public declaration, explaining how environmental information including

---

[26] For example, the declaration of DNI Negroponte states that "sources, methods, relationships, or targets" could cause harm by alerting "…adversaries that certain communications channels are secure…" Negroponte Decl. at ¶ 12. Looking behind this inadequate disclosure, as the Court is empowered to do, it would appear that the harm is already realized given that Qwest has openly disclosed that it refused to cooperate with the government because they concluded the government's request was illegal, making it plausible that an adversary "is alerted" to Qwest as a possible "secure channel." Markman Decl., Ex. 6.

chemical soil composition from a secret Air Force base could reveal activities, military capabilities, and the base location. The government explained the categories of information it sought to protect, and the harm that might result if the privilege was not invoked. At a minimum, the government must provide similar information here.

C. Congress Has Provided For Discovery In Electronic Surveillance Cases

This case should be allowed to move forward with non-privileged discovery, allowing the government an opportunity to object to particular discovery if and when it implicates specific state secret information. By objecting to specific discovery requests, the government may publicly specify how the request implicates state secrets and how those secrets might harm national security, if discovered.

By Act of Congress, Plaintiffs may take discovery, subject to all appropriate safeguards, to ascertain the legality of the electronic surveillance alleged in the Amended Complaint. 50 U.S.C. § 1806(f), 1845(f); *see* Section I.B.2.c, *supra*. This includes "contents" of the surveillance – that is, "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. §1801(n). Section 1806(f), therefore, gives Plaintiffs the right to take discovery about the legality of electronic surveillance of all of the alleged data-sources in this case (telephone content, call data records, and internet messages). This includes not only Plaintiffs' allegations concerning interception and disclosure of internet messages, but also concerning telephone calls and call data records (i.e., AT&T's disclosure of the "Daytona" database, including data about millions of calls made by AT&T customers, to the government). Plaintiffs' discovery will not be extensive – it will be enough to establish what AT&T did and whether it was illegal. And it can be done as needed pursuant to protective order, to avoid the disclosure of AT&T trade secrets.

Further, 50 U.S.C. §1845(f) gives Plaintiffs the right to discover information regarding pen registers or trap and trace devices used in AT&T's activities. Plaintiffs allege that AT&T is using such a device. *See* Amended Complaint ¶¶ 138–14 (Count VII). Information about the legality of AT&T's use of such devices goes to Plaintiff's claims regarding AT&T's interception

and disclosure of domestic telephone calls and email. Section 1845(f) also empowers the Court to permit Plaintiffs to take discovery regarding whether AT&T is providing a "live" feed of call data records to third parties like the government. This non-privileged discovery can and should proceed forthwith so that the Court can assess the ultimate issue in this case – the legality of the alleged electronic surveillance by AT&T.[27]

D. Specific Non-Secret Discovery Should Proceed

If the Court does not deny the government's alternative motion for summary judgment outright, the motion should be stayed under Fed. R. Civ. P. 56(f) until Plaintiffs have been allowed to adduce additional evidence through discovery. Of course, "Where … a summary judgment motion is filed so early in the litigation, before a party has had any realistic opportunity to pursue discovery relating to its theory of the case, district courts should grant any Rule 56(f) motion fairly freely." *Burlington N. & Santa Fe Ry. Co. v. The Assiniboine*, 323 F.3d 767, 773 (9th Cir. 2003); *Metabolife Int'l v. Wornick*, 264 F.3d 832, 846 (9th Cir. 2001). Given that discovery has not yet even commenced, this is such a case.

In the declaration submitted herewith, Plaintiffs make "(a) a timely application, which (b) specifically identifies (c) relevant information, (d) where there is some basis for believing that the information sought actually exists," under Rule 56(f) and thereby satisfy the Ninth Circuit's requirements for a stay of a summary judgment motion pending Rule 56(f) discovery. *VISA Int'l Serv. Ass'n v. Bankcard Holders of Am.*, 784 F.2d 1472, 1475 (9th Cir. 1986); Markman Decl., ¶¶ 10-20. The Rule 56(f) declaration sets out with specificity the non-secret discovery that Plaintiffs should be permitted to pursue in this case. Granting Plaintiffs' alternative Rule 56(f)

---

[27] Nor is the statutory regime created by Congress regarding discovery relating to electronic surveillance a one-way street. It also inures to the benefit of AT&T. Pursuant to 50 U.S.C. § 1806(f) and 1845(f), AT&T is permitted to engage in discovery relating to the legality of the surveillance in which it has played the central role. Given the law drafted by Congress and the availability of discovery subject to appropriate safeguards regarding the legality of the surveillance, dismissal is not a viable option.

motion would allow the discovery of further non-privileged evidence in the case, which may moot the government's assertion of the state secrets privilege.

The government may contend that some portions of such discovery are blocked by the state secrets privilege. Even assuming that is so, it is for the Court to determine, in the context of specific and concrete discovery disputes, whether and to what degree the state secrets privilege can be invoked to prevent a full adjudication of the substantial violations of basic rights that are at issue in this case. The government cannot so expand the state secrets privilege so that it eliminates without further inquiry all meaningful judicial review of Plaintiffs' claims.

CONCLUSION

For the reasons stated above, Plaintiffs respectfully request that the Court deny the government's motion to dismiss, and its alternative motion for summary judgment.

DATED: June 8, 2006

Respectfully submitted,

HELLER EHRMAN LLP
ROBERT D. FRAM (SBN 126750)
robert.fram@hellerehrman.com
MICHAEL M. MARKMAN (SBN 191388)
michael.markman@hellerehrman.com
ETHAN C. GLASS (SBN 216159)
SAMUEL F. ERNST (SBN 223963)
NATHAN SHAFROTH (SBN 232505)
ELENA DIMUZIO (SBN 239953)
333 Bush Street
San Francisco, CA 94104
Telephone: 415/772-6000
415-772-6268 (fax)

ROBERT D. FRAM

Attorneys for Plaintiffs

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN
LEE TIEN
KURT OPSAHL
KEVIN S. BANKSTON
CORYNNE MCSHERRY
JAMES S. TYRE
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333

LERACH COUGHLIN STOIA GELLER RUDMAN & ROBBINS LLP
REED R. KATHREIN
JEFF D. FRIEDMAN
SHANA E. SCARLETT
MARIA V. MORRIS
100 Pine Street, Suite 2600
San Francisco, CA 94111
Telephone: 415/288-4545
415/288-4534 (fax)

LERACH COUGHLIN STOIA GELLER
RUDMAN & ROBBINS LLP
ERIC ALAN ISAACSON
655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)

TRABER & VOORHEES
BERT VOORHEES (137623)
bv@tvlegal.com
THERESA M. TRABER (116305)
tmt@tvlegal.com
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103
Telephone: 626/585-9611
626/ 577-7079 (fax)

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: 415/433-3200
415/433-6382 (fax)

CERTIFICATE OF SERVICE

I hereby certify that on June 20, 2006, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the attached Electronic Mail Notice List, and I hereby certify that I have mailed the foregoing document or paper via the United States Postal Service to the following non-CM/ECF participants:

David W. Carpenter
Sidley Austin Brown & Wood LLP
Bank One Plaza
10 South Dearborn Street
Chicago, IL 60600

David L. Lawson
Sidley Austin Brown & Wood
172 Eye Street, N.W.
Washington, DC 20006

By /s/
Cindy A. Cohn, Esq. (SBN.145997)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993
cindy@eff.org