Susan Freiwald, *Pro Hac Vice*
NY Reg. No. 2557627
Professor of Law
UNIVERSITY OF SAN FRANCISCO SCHOOL OF LAW
2130 Fulton Street
San Francisco, California 94117-1080
Telephone: (415) 422-6467
Email: freiwald@usfca.edu

In Pro Se as Amicus Curiae

Lauren Gelman, State Bar No. 228734
Jennifer Stisa Granick, State Bar No. 168423
STANFORD LAW SCHOOL
CYBERLAW CLINIC
CENTER FOR INTERNET & SOCIETY
Crown Quadrangle
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 724-3358
Facsimile: (650) 723-4426
Email: gelman@stanford.edu

Attorneys for Amicus Curiae Law Professors

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL, and ERIC KNUTZEN On Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. AT&T CORPORATION, AT&T INCORPORATED, and DOES 1-2, Inclusive, Defendants.	Case No.: C 06-0672-VRW **BRIEF OF AMICUS CURIAE LAW PROFESSORS IN SUPPORT OF PLANTIFFS' OPPOSITION TO NOTICE OF MOTION AND MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA** Hearing Date: June 21, 2006 Judge: The Hon. Vaughn R. Walker Courtroom: 6, 17th Floor

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

Proposed Amici Curiae Law Professors ("Amici") are law professors whose scholarship, teaching, and practice focus on electronic surveillance and constitutional law. *Amici* wish to highlight for the Court the historical role the judicial branch has played in regulating surveillance and to show that the information necessary to prove or defend against Plaintiffs interception claims is publicly known and not protected by the state secrets privilege.

Amici are:

Susan Freiwald
Professor of Law
UNIVERSITY OF SAN FRANCISCO SCHOOL OF LAW

Cynthia R. Farina
Associate Dean of the University Faculty
Professor of Law
CORNELL SCHOOL OF LAW

Peter M. Shane
Director, Center for Interdisciplinary Law and Policy Studies, and
Joseph S. Platt, Porter, Wright, Morris & Arthur Professor of Law
OHIO STATE UNIVERSITY
MORITZ COLLEGE OF LAW

Peter Raven-Hansen
Glen Earl Weston Research Professor of Law
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL

Erwin Chemerinsky
Alston & Bird Professor of Law and Political Science
DUKE UNIVERSITY

SUMMARY OF ARGUMENT

Amici, law professors who specialize in electronic surveillance and constitutional law, urge this Court to protect the judicial branch's role in overseeing electronic surveillance and to hold accountable Defendant telecommunications companies for their failure to protect their subscribers' privacy. Federal law strictly prohibits interception of communications without a

court order. It requires that telecommunications providers refuse to help the government listen in to citizens' communications without a court's approval. When it set up the statutory scheme, Congress recognized that telecommunications providers play a critical role in protecting subscribers' privacy interests. In contrast to those whose houses are searched, victims of electronic surveillance rarely learn that someone has listened to their telephone conversations without authorization. For that reason, Congress tasked telecommunications providers with ensuring that any surveillance is properly authorized, and provided strict penalties for ignoring that responsibility. This case is about whether the Defendants violated their obligations under the law.

The Government asks this Court to disrupt this statutory scheme and to decline to decide whether the telecommunications companies violated the law because the case implicates state secrets. However, at least the interception claims, and perhaps all the claims, may be decided based on publicly available information. If Defendants intercepted Plaintiffs' conversations without a court order, they violated federal electronic surveillance law. Liability attaches regardless of what Defendants did with the information afterwards. While the government's role in these interceptions may be an important part of the public discourse about this case, the government's actions are not implicated in the interception claims.

As we enter a digital era, more and more of citizens' most private information passes through the hands of telecommunications companies like Defendants to whom the government and others will turn when they want information. Constitutional and federal statutory law explicitly requires the judicial branch's engagement in that process – both to pre-approve government requests for information and to remedy situations when the government fails to obtain that approval and the telecommunications companies provide the information nonetheless. In this case, Plaintiffs allege that the government failed to obtain pre-surveillance review, yet the Defendants will avoid liability if this Court dismisses this case. *Amici* urge this Court to deny the Government's request and reaffirm the role of the judicial branch in oversight of all aspects of electronic surveillance.

///

ARGUMENT

I. EVALUATING PLAINTIFFS' CLAIMS OF UNLAWFUL INTERCEPTION DOES NOT REQUIRE DISCLOSURE OF STATE SECRETS

Plaintiffs allege that AT&T Corp. and AT&T Inc. (collectively "AT&T" or "Defendants") unlawfully disclosed wire and electronic communications to the government in violation of 18 U.S.C. § 2511(1)(a). Neither the elements of the statutory offense nor the available defenses require disclosure of material that is currently unavailable to the public. Section 2511(1)(a) prohibits anyone from intentionally intercepting a wire, oral or electronic communication. To defend Plaintiffs' claims that Defendants violated this prohibition, Defendants have three options.[1] They can dispute the evidence provided by Plaintiffs' Declarant Mark Klein and allege that they did not engage in wholesale interceptions of their subscribers' information. Or they can acknowledge the interceptions, but claim that they acted pursuant to a court order obtained pursuant to 18 U.S.C. § 2518 or that they relied on an invalid court order in good faith under 18 U.S.C. § 2520(d). The two latter defenses require that there be a "piece of paper" this Court can examine to determine whether the Defendants have a valid defense. If not, they violated the law. This finding, while perhaps requiring an *in camera* review of the "piece of paper," does not present "a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." *United States v. Reynolds*, 345 U.S. 1, 10 (1953).

A. Proving Defendants Intercepted Their Subscribers' Communications Does Not Disclose State Secrets

The first question is whether Defendants intercepted their subscribers' communications. An interception happens at the moment a communication is copied. *United States v. Rodriguez*, 968 F.2d 130, 136 (2nd Cir. 1992). The statute is violated when someone intercepts a communication regardless of what they subsequently do with the contents of the

[1] Defendants could establish that they fit into one of the statutory exceptions under 18 U.S.C. § 2511(2), but none of those applies to the surveillance alleged in this case. *See* Plaintiffs' Amended Notice of Motion and Motion for Preliminary Injunction, April 5, 2006, at 19-22.

communication they intercepted. See *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978); *United States v. Councilman* 418 F.3d 67, 84 (1st Cir. 2005). In this case, Defendants' liability under § 2511(1)(a) arises from their interception of Plaintiffs' communications without a court order. It is irrelevant for purposes of determining Defendants' liability to whom they provided the communications, or what the recipient did with the information. This Court does not need to know what information, if any, was turned over to the government, or how the government used the information, to find Defendants liable under § 2511(1)(a).

There is significant evidence before the Court that Defendants intercepted some of their subscribers' communications. Plaintiffs' witness Mark Klein describes in his declaration Defendants' wholesale surveillance of their subscribers' telephone calls, electronic mail, and internet use. Brief of Amicus Curiae Mark Klein at 4-5. He states that for some subscribers, Defendants' ongoing practice was to copy the entire flow of the communications traffic to which they had access. Id. The activities Klein describes took place on Defendants' premises and were performed by Defendants' employees on Defendants' equipment. The alleged violations occurred at the moment Defendants captured or redirected the contents of the Plaintiffs' communications. As the Second Circuit has explained, "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time." *United States v. Rodriguez*, 968 F.2d at 136. Because an interception occurs at the moment a communication is copied, Plaintiffs need do no more than establish copying to make out a viable claim under 18 U.S.C. § 2511. [2]

Defendants are liable regardless of what they subsequently did with any of the communications they intercepted. See *Jacobson v. Rose*, 592 F.2d at 522. It is irrelevant to Plaintiffs' interception claims that the National Security Agency ("NSA") was purportedly the

[2] *Amici* focus on the Wiretap Act and the Electronic Communications Privacy Act rather than FISA because the nature of the plaintiff class, which excludes agents of foreign powers and terrorist operatives, is such that Plaintiffs are improper FISA targets. *See* 50 U.S.C. § 1804 (4) (describing targets as foreign powers or agents of foreign powers).

party that received the copies of the intercepted communications and what the NSA might have allegedly done with the communications thereafter. The law asks only if there was an intentional interception of a wire, oral, or electronic communication. For example, in *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005), the defendant, an officer who worked for an electronic communications service provider, made copies of his subscribers' emails in order to learn about his competitor's business practices, and stored those emails in a file on company computers. The First Circuit, *en banc*, held that the defendant violated 18 U.S.C. § 2511 because he intercepted his subscribers' communications without either a court order or an applicable exception. Whether or not Councilman subsequently used the communications he obtained was irrelevant to his criminal liability. The violation occurred at the point of unlawful interception. See *Councilman*, 418 F.3d at 84 ("'[E]lectronic communications,' which are defined expansively, may not be 'intercepted'.") (quoting 18 U.S.C. § 2511(1)(a)). Similarly, in this case, it does not matter to the interception claim that the Defendants allegedly forwarded the communications to the NSA. It is the capture of the information itself, not the forwarding, which the statute prohibits.

The Government's argument that it would be required to confirm or deny the existence, scope and potential targets of its alleged intelligence activities if this Court were to adjudicate Plaintiffs' claims is therefore in error. The Government's involvement in Defendants' activities, if any, is irrelevant to Plaintiffs' ability to establish that Defendants intercepted Plaintiffs' communications. Plaintiffs, the public, and *amici* are aware that telecommunications carriers like Defendants have both the capability and often the legal responsibility to intercept communications, and that the government often asks them to do so. That is no secret. The issue is whether Defendants did so without authorization here. Defendants could counter Mark Klein's declaration with evidence showing that Defendants did not engage in the particular interceptions alleged in this case. There is no need to disclose state secrets to prove or disprove Plaintiffs' allegations. Therefore, the Court should not dismiss this case as the Government requests.

B. Proving Defendants Have a Valid Defense for Intercepting Their Subscribers' Communications Does Not Require Disclosure of State Secrets

If Defendants do not dispute Plaintiffs' allegations that they violated 18 U.S.C. § 2511(1)(a), they may defend their actions by establishing that they acted pursuant to a court order under 18 U.S.C. § 2518.[3] In the absence of a valid court order, Defendants may produce an invalid court order that they relied upon in good faith. *See* 18 U.S.C. § 2520(d). If Defendants are unable to establish either of these, then they are liable to Plaintiffs for damages, subject to injunctive relief, and vulnerable to criminal charges. *See* 18 U.S.C. §§ 2511(4)(a), 2520. Proving either of these defenses requires the Defendants to produce a court order. An *in camera* review of that order would not disclose state secrets, and therefore this case should not be dismissed.

Section § 2511(2)(a)(ii) authorizes a provider "to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral or electronic communications … if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with – (A) a court order directing such assistance signed by the authorizing judge… setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required." Government agents may ask the court that grants their interception order under procedures specified in 18 U.S.C. § 2518 to include in the order a direction to the provider to give assistance. Such court orders must also contain detailed information about the nature of the investigation, the target, and the communications sought, and must specify the period of time during which the investigation is authorized. *See* 18 U.S.C. § 2518(4). To the extent the court order contains information that may be considered sensitive, a court could accept it under seal and then redact as necessary to protect against disclosure of that information.[4]

---

[3] They could also produce a court order under FISA, 50 U.S.C. § 1804, but *see* note 1.

[4] The administration has conceded that its domestic surveillance program has operated without the benefit of court orders, *see* Plaintiffs' Request for Judicial Notice, March 31, 2006, pp. 4-5, so it is unlikely that any court orders authorized the interceptions in this case.

Electronic surveillance law clearly required Defendants to base any interceptions of their subscribers' communications on a court order. The court order requirement serves an important function. Telecommunications carriers like the Defendants stand as the only barrier between the government's desire to obtain private communications and their subscribers' right to privacy in those communications. That is why the law places a heavy burden on these companies to permit violations of their customers' privacy only when the government couples its request for an interception with an independent and impartial arbiter's assessment that the privacy violation is warranted.

Though the statutory scheme seeks to enforce checks and balances on the executive branch, the law focuses on the actions of AT&T Corp. and AT&T Inc., not on the actions of the government. It does not matter whether the government's reason for requesting the information may implicate state secrets. Defendants still needed to demand a court order, and whether or not they had one does not implicate state secrets. If Defendants do not rebut the allegation that they intercepted their subscribers' communications, and if they have no valid defense, then they should be held liable – as the statute requires. 18 U.S.C. § 2511(1)(a).

II. ESTABLISHED CONSTITUTIONAL AND STATUTORY LAW MANDATE JUDICIAL REVIEW OF ELECTRONIC SURVEILLANCE

The Government claims that "no aspect of this case can be litigated without disclosing state secrets." Government's Response to Plaintiffs' Memorandum of Points and Authorities, May 24, 2006, p. 1. The Government's assertion of state secrets is implausibly expansive given that this Court may consider Plaintiffs' interception claims without divulging state secrets, as discussed in Part I, *supra*. As to Plaintiffs' other claims, however, *amici* cannot fully address the Government's assertion, because we have limited access to facts the Government has presented to the Court .[5] Nonetheless, the history of electronic surveillance

[5] Plaintiffs raise claims pertaining to stored communications and communication records, as well as claims arising under state law, the Foreign Intelligence Surveillance Act (FISA), 47 U.S.C. § 605, and the Fourth and First Amendments. Establishing the constitutional claims,

regulation and established law require that this Court scrutinize closely the Government's claims of privilege. It may be that the states secret privilege does not apply to most, or even any, of the Plaintiffs' claims.[6] To the extent the Government demands dismissal based on other considerations, such as a concern with keeping NSA's operations secret, those policy concerns should yield, if at all possible, to long established constitutional and statutory doctrine under which the judicial branch must conduct meaningful review of electronic surveillance at all stages.

This country has a long history of judicial oversight of the executive branch's power to invade the privacy of American citizens. A dismissal here will prevent judicial review of an allegedly vast program that invades the privacy of millions of Americans. This result stands in sharp contrast to the privacy protections the law grants citizens in their conversations.

State secrets doctrine recognizes the radical effect of preventing judicial review when the privilege is invoked. It therefore requires a court to consider the plaintiffs' "showing of necessity" when it determines "how far [to] probe in satisfying itself that the occasion for invoking the privilege is appropriate. Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted … ." *United States v. Reynolds, supra* at 11. In this case, the showing of necessity could not be stronger – it is the firmly established need for judicial checks and balances on the executive branch's use of electronic surveillance. If there is any way that this case can go forward without compromising state secrets, then it should.

///

///

///

---

for example, requires proving state action. That requires evidence about the Government's role in interception that the section 2511 claim does not..

[6] Both Director of National Intelligence Negroponte and Lieutenant General Alexander assert a state secrets privilege as to only certain of the information implicated by Plaintiffs' claims. *See* Declaration of John D. Negroponte at 4, Declaration of Lieutenant General Keith B. Alexander at 2-3.

A. Judicial Review of Electronic Surveillance Provides an Essential Check on Executive Power

The executive branch has consistently tried to evade any restrictions on its electronic surveillance, since the first federal statute prohibiting interception of communications was passed. When Section 605 of the Communications Act of 1934, which prohibited wiretapping, was enacted, federal agents argued that they were immune from the flat prohibition that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence contents, substance, purport, effect or meaning of such intercepted communication to any person." Communications Act of 1934, ch. 652, 48 Stat. 1064, 1100 (codified at 47 U.S.C. § 605 (1958) (*amended* 1968)). The Supreme Court, however, squarely rejected government immunity in *Nardone v. United States*, 302 U.S. 379, 382 (1937), when the Court rejected the government's use of wiretap-derived evidence in court. The Court construed the statute's "plain words" and "clear language" to find that its prohibition applied to the government. *Id*.

Over the next thirty years, government lawyers made other unsuccessful attempts to avoid the law's restrictions. They argued, for example, that so long as state agents provided them with wiretap-derived information, federal agents could use it in court. The Supreme Court renounced that practice in 1957. See *Benanti v. United States*, 355 U.S. 96, 100 (1957). Although the Court during this period issued decisions that reinforced the federal prohibition against wiretapping, some contemporary commentators saw a reversal of *Olmstead v. United States*, 277 U.S. 438 (1928), that would bring Fourth Amendment protection to surveillance targets, as the only way to rein in executive branch surveillance. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Alabama L. Rev. 9, 26-31 (2004) (describing the history and current form of electronic surveillance law).

When *Katz v. United States*, 389 U.S. 347 (1967), finally found electronic surveillance to implicate the Fourth Amendment, a protracted public debate raged about how to regulate it. Many people maintained that the risks of abuse inherent in electronic surveillance required Congress to ban it entirely. A middle group, including President Johnson, his Attorney General and twenty-one senators, approved of electronic surveillance, strictly regulated, when

used solely to protect national security. The ultimate decision was to permit electronic surveillance only for national security and law enforcement purposes in the Wiretap Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212, subject to a comprehensive scheme that carefully circumscribes the use of electronic surveillance by government and private parties alike. *See* Freiwald, 56 Alabama L. Rev. at 13-14, 23-24.[7]

Since then, executive branch surveillance has been carefully delimited. For example, when the executive branch advocated the surveillance of domestic threats to national security without a warrant, the Supreme Court rejected that power, although it did not address foreign threats. *See United States v. United States District Court*, 407 U.S. 297 (1972) ("*Keith*"). In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") in response to reports that the executive branch was abusing its power to conduct foreign intelligence surveillance. *See* 50 U.S.C. §§ 1801-1811. Together, FISA and the Wiretap Act entirely prohibit warrantless electronic surveillance in the United States except for no more than a few days in an emergency, *see* 50 U.S.C. § 1805(f), 18 U.S.C. § 2518(7), and no more than two weeks in the immediate aftermath of the declaration of war. *See* 50 U.S.C. § 1811.

Despite the long history of the judiciary's statutory and constitutional obligation to police surveillance, the Government asks this Court to take the radical step of dismissing the case and preventing any judicial remedy for the statutory violations alleged. Moreover, when a state actor conducts the surveillance, as alleged in this case, then the requirement of judicial review has the added weight of the Fourth Amendment. Because Plaintiffs' class excludes foreign powers, agents of foreign powers, and "anyone who knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore," (Amended Complaint, Feb. 22, 2006, ¶ 70), Plaintiffs are entitled to the highest protections of the federal surveillance laws and the Constitution. See, e.g., *Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986) (Scalia, Circuit Justice).

---

[7] Courts have upheld the constitutionality of the Wiretap Act. See *United States v. Donovan*, 429 U.S. 413, 429 n. 19 (1977); *United States v. Tortorello*, 480 F.2d 764, 773 (2nd Cir. 1973), *cert. denied*, 414 U.S. 866 (1973).

The Supreme Court has clearly established that the Fourth Amendment requires judicial review of executive branch surveillance practices. "The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Keith*, 407 U.S. at 317. In fact, after the majority described the high hurdles executive branch agents would have to overcome before their surveillance could pass constitutional muster in *Berger v. New York*, 388 U.S. 41 (1967), two dissenters accused the majority of trying to prohibit eavesdropping altogether. See *Berger*, 388 U.S. at 71 (Black, J., dissenting); *id*. at 111 (White, J., dissenting) (invalidating a state eavesdropping statute as an unconstitutional general warrant).

Electronic surveillance laws require judges to approve electronic surveillance before it starts, review it as it continues and when it ends, and provide a forum for victims of unlawful surveillance. Defendants and the Government have not claimed that they secured judicial approval to conduct the surveillance at issue, even though the evidence suggests the surveillance has spanned several years. If this case is dismissed, no such review will ever take place. When Plaintiffs ask the Court to remedy violations of their established constitutional and statutory rights, they present the Court with the first and last opportunity to review Defendants' surveillance practices.

The executive branch cannot rewrite electronic surveillance law, as it asks this Court to do, to prevent judicial oversight of cases where national security issues are at stake. In *Berger v. New York*, 388 U.S. 41 (1967), the Supreme Court established the constitutional requirements for any statute that purported to authorize law enforcement's use of electronic surveillance. To avoid giving investigators a "roving commission" to search any and all conversations, the *Berger* court required applications for court orders not just to establish probable cause but also to identify both the person targeted and the conversations sought. *Berger*, 388 U.S. at 59. In addition to the active involvement of a judge in granting court orders, the Court required that the warrant be returned to the granting judge, so that the officer alone would not decide how to use any conversations seized. Overall, the Court emphasized

the need for "adequate judicial supervision or protective procedures." *Berger*, 388 U.S. at 60. Six months later, in *Katz*, 389 U.S. 347 the Court affirmed that victims of unlawful surveillance would be afforded suppression remedies so that after-surveillance review could ensure that officers had complied with the Fourth Amendment requirements.

When Congress passed the Wiretap Act, it codified and elaborated the constitutional requirements the Supreme Court had just established. The statutory scheme provides for the active involvement of a reviewing court at all stages. Pre-surveillance, the reviewing judge must first determine that "normal investigative procedures" not involving electronic surveillance will be inadequate and that there is probable cause to believe that the surveillance will obtain incriminating evidence about the targets' commission of a particular enumerated offense. During the surveillance, the Court must approve any extensions to the order, which may not last more than thirty days. The reviewing court must receive any recordings of the surveillance when it is terminated and then determine to whom to provide notice, in addition to the target himself. 18 U.S.C. § 2518. Finally, the statute added a statutory exclusionary rule to deter unlawful law enforcement practices. 18 U.S.C. § 2515. Generous civil and equitable remedies and strict criminal penalties further demonstrate Congress' commitment to eradicating unlawful surveillance by the government and private parties. *See* 18 U.S.C. §§ 2511, 2520.

The special scheme Congress designed to address electronic surveillance reflects the unusual threat to privacy that such surveillance poses. As the several Courts of Appeals that considered how to regulate silent video surveillance in the mid-1980s and early 1990s explained, electronic surveillance practices require a heightened level of judicial oversight. Compared to one-shot physical searches for which a traditional warrant usually suffices, electronic surveillance is intrusive, continuous, hidden and indiscriminate. In other words, electronic surveillance divulges a wide range of private information over a significant period of time, unbeknownst to the target of that surveillance. For that reason, several federal appellate courts agreed that government video surveillance must be subject to the core protective features of the Wiretap Act to ensure that surveillance practices do not unduly

intrude on privacy rights.[8] See, e.g., *United States v. Torres*, 751 F.2d 875, 882-884 (7th Cir. 1984); *United States v. Biasucci*, 786 F.2d 504 (2nd Cir. 1986); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir.1992) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992).

The surveillance practices that the Plaintiffs allege in this case clearly match the description that the Courts of Appeals used to characterize video surveillance. Whether the surveillance involves the wiretapping of traditional telephone calls, the interception of emails, or the acquisition of information about subscribers' activities online, in each case such surveillance is intrusive, continuous, hidden and indiscriminate. The surveillance the Plaintiffs describe demands more than a traditional warrant and certainly does not qualify for an exception to the warrant procedure. The Government's discussion of cases that dispensed with the warrant requirement is therefore inapposite.

It would upset the constitutional balance and flout established federal law to permit the executive branch to be the sole arbiter of the legality of the surveillance alleged in this case. In fact, Congress and the courts have cut off the very path that the Government is trying to go down by having this case dismissed. This Court should fulfill its obligations under the law and hear this case.

B. Careful Scrutiny of the Government's Claimed Privileges May Demonstrate that this Court Can Review Plaintiffs' Claims Without Endangering State Secrets

If Plaintiffs' communications were the targets of surveillance that did not meet constitutional and statutory requirements, then the Government may not use the state secrets privilege to conceal those illegal actions. This Court must examine the elements and defenses of each allegation made by Plaintiffs and parse the Government's state secrets claim to determine whether state secrets privileged information is necessary to prove or disprove any

[8] The Courts of Appeal have applied the following requirements of the Wiretap Act to government video surveillance in which the target had a reasonable expectation of privacy: that the surveillance is used as a last resort, that agents minimize the interception of non-incriminating images, and that applications satisfy the particularity requirement. *See* Freiwald, 56 Alabama Law R. at 9, 72-73.

element or defense. See *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983) ("[W]henever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.").

The Court should not dismiss this case and leave the Plaintiffs without any recourse for the Defendants' illegal actions unless the Government can describe exactly how state secrets will be disclosed by a full airing of the Defendants' actions in regard to Plaintiffs' communications.

In its publicly available pleadings, the Government expresses concern that litigating Plaintiffs' case risks disclosure of intelligence-gathering sources and methods or capabilities.[9] In particular, the Government states that "[a]djudicating each claim in the Amended Complaint would require confirmation or denial of the existence, scope, and potential targets of alleged intelligence activities, as well as AT&T's alleged involvement in such activities." Government's Motion to Dismiss, May 13, 2006, p. 16. Because of the paucity of responsive information from the Defendants and the limitation on *amici's* access to the Government's arguments, *amici* cannot fully analyze the Government's claim.

However, most of the facts that the Government expresses concern about revealing were in the public domain well before this case. The public has long been aware that the NSA conducts signals intelligence on domestic telecommunications systems. It can hardly surprise anyone that the Defendants, two large telecommunications carriers, would be involved in those programs. Top administration officials have conceded the existence of NSA surveillance in general, and the "Terrorist Surveillance Program" in particular. *See, e.g.* Eggen and Pincus, *Campaign to Justify Spying Intensifies*, Washington Post, January 24, 2006, page A04, available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/01/23/AR2006012300754.html . In addition, it is difficult to see

[9] In its public materials, the Government does not claim that Plaintiffs' case risks the disruption of diplomatic relations with foreign governments or otherwise impairs the nation's defense capabilities, which are the other two typical grounds for state secrets. See, e.g., *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983).

how Plaintiffs' claims would relate to the scope and targets of any such programs. To make out a Fourth Amendment violation, for example, Plaintiffs must demonstrate that a government actor or agent seized communications in which the speaker invested a reasonable expectation of privacy. Who exactly the NSA targeted in its Terrorist Surveillance Program is not relevant to the Plaintiffs' claims. The Government misapprehends its burden of proof to the extent it suggests that it could refute Plaintiffs' evidence that they were victims of surveillance merely by asserting that Plaintiffs were not members of the target group and therefore could not have been surveilled. A mere assertion that Plaintiffs were not contemplated by a particular program's design does not rebut proof that Plaintiffs' constitutionally protected communications were nonetheless intercepted.

If the Government raises legitimate concerns about particular technological sources and methods, then an approach similar to that under the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. III, § 1 *et seq.*, could permit the court to consider classified materials *in camera*. In *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001), the court applied CIPA to learn, *ex parte*, about the operation of a key logger system ("KLS") that FBI agents had installed to obtain the defendant's passphrases for his encrypted files. The court determined, from the FBI's *in camera* presentation, attended by persons with top-secret clearance only, that the KLS does not "intercept" under the definition of that term in the Wiretap Act.[10] The court provided defense counsel with an unclassified summary of the technology "sufficient to allow the defense to effectively argue the motion to suppress." *Scarfo*, 180 F. Supp. 2d at 576. Similar procedures, if needed to protect national security, could be employed in this case. What is not needed is the blanket dismissal of claims just because they may implicate classified sources and methods for their resolution. See *Ellsberg v. Mitchell*, *supra* at 57. ("Thus the privilege may not be used to shield any material not strictly necessary to prevent injury to national security….").

[10] *Amici* discuss this case not to approve of its reasoning but to illustrate a procedure for handling classified surveillance methods without disclosing them to the public.

Plaintiff's case differs significantly from the recent state secrets case upon which the Government relies. In *El-Masri v. Tenet*, No. 1:05cv1417, (E.D. Va. May 12, 2006), the Government sought "to protect from disclosure the operational details of the extraordinary rendition program" when "a public admission of the alleged facts would obviously reveal sensitive means and methods of the country's intelligence operations." Slip. Op. at 11. In this case, by contrast, the actions of the telecommunications carriers, not the government, are at issue. Unlike the classified and clandestine intelligence program that involved foreign intelligence services at issue in *El-Masri*, Plaintiffs here challenge the actions of domestic telecommunications carriers in the United States. Moreover, it is public knowledge that telecommunications companies cooperate with the government to disclose the contents of citizen's communications. Plaintiffs are not looking for operational details that describe how the government is using the information it receives from the Defendants. If Defendants were doing wholesale interception of everyone's calls, then Plaintiffs do not need to know who is targeted, what information the government obtains, how the information is transferred, or what the government does with it in order to succeed in their claims against Defendants.

The "secret" nature of the information at issue in this case, contrary to the hyperbolic language that permeates the Government briefs, could, on careful inspection, be quite limited. The interception claim, for example, may be adjudicated without implicating national security. To the extent that the Government asserts a valid state secrets privilege over some aspects of the case, the rest of the case should nonetheless proceed, with procedures to protect classified documents, if necessary. Any lesser claim of privilege should yield in the face of the overwhelming policy favoring judicial review of electronic surveillance.[11] "[I]t is well settled that 'dismissal is appropriate only when no amount of effort and care on the part of the court and the parties will safeguard privileged material.'" *El-Masri*, slip op. at 12 (quoting

[11] The Government appears to claim that a privilege over matters relating to NSA operations requires dismissal. *Amici* point out that if that privilege alone required dismissal, it would open up a giant hole in the electronic surveillance laws. Government agents could immunize their surveillance practices from judicial review by somehow involving the NSA in them. That cannot be what Congress had in mind.

Sterling v. Tenet, 416 F.3d 338, 348 (4th Cir. 2005)). This Court should not dismiss Plaintiffs' case. Instead, it should require the Defendants' actions to undergo the judicial scrutiny that history, the Constitution and federal statutes require.

CONCLUSION

The Court should reject the Government's argument that the Judicial Branch has no role to play in determining whether the telecommunications companies violated the Constitution and federal law as Plaintiffs allege. The weighty interests favoring judicial review and the large scale of the electronic surveillance that Plaintiffs allege require the Court to scrutinize carefully the Government's claim of a state secrets privilege. The claims alleging interceptions, for example, present no state secrets concern. To the extent the Court determines that some information in the case is subject to the state secrets privilege, it must try to disentangle that information from the rest of the case and proceed with what remains. This Court should summarily dismiss the Government's attempt to extend the privilege to cover those aspects of the case that are not state secrets but that merely raise a risk of disclosing confidential information, particularly when the Court could protect that confidential information. Because at least some of Plaintiffs' claims do not implicate state secrets, the Court should reject the Government's request for dismissal. Dismissal of this case would irrevocably compromise the judiciary's role. The Court would not be able to serve as a check on executive surveillance of American citizens or to ensure that telecommunications carriers protect customer privacy as the law requires.

///

///

///

///

Dated: June 16, 2006

Respectfully submitted,

By: /S/ Susan Freiwald
Susan Freiwald, *Pro Hac Vice*
Voice: (415) 422-6467
Email: freiwald@usfca.edu

UNIVERSITY OF SAN FRANCISCO SCHOOL OF LAW
2130 Fulton Street
San Francisco, CA 94117-1080

In Pro Se as Amicus Curiae

By: /S/ Lauren A. Gelman
Lauren A. Gelman
Voice: (650) 724-3358
Email: gelman@stanford.edu

By: /S/ Jennifer S. Granick
Jennifer S. Granick
Voice: (650) 724-0014
Email: jennifer@granick.com

STANFORD LAW SCHOOL
CENTER FOR INTERNET & SOCIETY
CYBERLAW CLINIC
Crown Quadrangle
559 Nathan Abbott Way
Stanford, California 94305-8610

Attorneys for Intervenor Plantiffs
Amici Curiae Law Professors