

1 Susan Freiwald, *Pro Hac Vice*
2 NY Reg. No. 2557627
3 Professor of Law
4 UNIVERSITY OF SAN FRANCISCO SCHOOL OF LAW
5 2130 Fulton Street
6 San Francisco, California 94117-1080
7 Telephone: (415) 422-6467
8 Email: freiwald@usfca.edu

9 *In Pro Se as Amicus Curiae*

10 Lauren Gelman, State Bar No. 228734
11 Jennifer Stisa Granick, State Bar No. 168423
12 STANFORD LAW SCHOOL
13 CYBERLAW CLINIC
14 CENTER FOR INTERNET & SOCIETY
15 Crown Quadrangle
16 559 Nathan Abbott Way
17 Stanford, California 94305-8610
18 Telephone: (650) 724-3358
19 Facsimile: (650) 723-4426
20 Email: gelman@stanford.edu

21 *Attorneys for Amicus Curiae Law Professors*

22 UNITED STATES DISTRICT COURT
23 NORTHERN DISTRICT OF CALIFORNIA
24 SAN FRANCISCO DIVISION

25 TASH HEPTING, GREGORY HICKS,)
26 CAROLYN JEWEL, and ERIC KNUTZEN)
27 On Behalf of Themselves and All Others)
28 Similarly Situated,)
29 Plaintiffs,)
30 v.)
31 AT&T CORPORATION, AT&T)
32 INCORPORATED, and DOES 1-2,)
33 Inclusive,)
34 Defendants.)

Case No.: C 06-0672-VRW

**BRIEF OF AMICUS CURIAE LAW
PROFESSORS IN SUPPORT OF
PLAINTIFFS' 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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page

INTEREST OF THE AMICI CURIAE 1

SUMMARY OF ARGUMENT 1

ARGUMENT 3

 I. EVALUATING PLAINTIFFS’ CLAIMS OF UNLAWFUL INTERCEPTION DOES NOT REQUIRE DISCLOSURE OF STATE SECRETS 3

 A. Proving Defendants Intercepted Their Subscribers’ Communications Does Not Disclose State Secrets..... 3

 B. Proving Defendants Have a Valid Defense for Intercepting Their Subscribers’ Communications Does Not Require Disclosure of State Secrets 6

 II. ESTABLISHED CONSTITUTIONAL AND STATUTORY LAW MANDATE JUDICIAL REVIEW OF ELECTRONIC SURVEILLANCE 7

 A. Judicial Review of Electronic Surveillance Provides an Essential Check on Executive Power..... 9

 B. Careful Scrutiny of the Government’s Claimed Privileges May Demonstrate that this Court Can Review Plaintiffs’ Claims Without Endangering State Secrets 13

CONCLUSION..... 17

TABLE OF AUTHORITIES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page

CASES

Benanti v. United States, 355 U.S. 96 (1957) 9
Berger v. New York, 388 U.S. 41 (1967) 11, 12
Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983) 14
El-Masri v. Tenet, No. 1:05cv1417, (E.D. Va. May 12, 2006)..... 16
Halperin v. Kissinger, 807 F.2d 180 (D.C. Cir. 1986) 10
Jacobson v. Rose, 592 F.2d 515 (9th Cir. 1978)..... 4
Katz v. United States, 389 U.S. 347 (1967) 9, 12
Nardone v. United States, 302 U.S. 379 (1937)..... 9
Olmstead v. United States, 277 U.S. 438 (1928) 9
Sterling v. Tenet, 416 F.3d 338 (4th Cir. 2005) 17
United States v. Biasucci, 786 F.2d 504 (2nd Cir. 1986)..... 13
United States v. Councilman 418 F.3d 67 (1st Cir. 2005) 4, 5
United States v. Donovan, 429 U.S. 413 (1977)..... 10
United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992)..... 13
United States v. Reynolds, 345 U.S. 1 (1953)..... 3
United States v. Rodriguez, 968 F.2d 130 (2nd Cir. 1992)..... 3, 4
United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) 15
United States v. Torres, 751 F.2d 875 (7th Cir. 1984)..... 13
United States v. Tortorello, 480 F.2d 764 (2nd Cir. 1973)..... 10
United States v. United States District Court, 407 U.S. 297 (1972)..... 10, 11

STATUTES

United States Constitution
 Amendment I 8
 Amendment IV *passim*

Title 18 United States Code, et seq.
 18 U.S.C. App. III, § 1 *et seq.*, (*Classified Information Procedures Act*) 15
 18 U.S.C. § 2511 4, 5, 8, 12
 18 U.S.C. § 2511(1)(a)..... 3, 4, 5, 6, 7
 18 U.S.C. § 2511(2) 3
 18 U.S.C. § 2511(2)(a)(ii)..... 6
 18 U.S.C. § 2511(4)(a)..... 6
 18 U.S.C. § 2515 12
 18 U.S.C. § 2518 3, 6
 18 U.S.C. § 2518(4) 6
 18 U.S.C. § 2518(7) 10
 18 U.S.C. § 2520 6, 12
 18 U.S.C. § 2520(d) 3, 6

Title 47 United States Code, et seq.

47 U.S.C. § 605 (*Foreign Intelligence Surveillance Act*) 4, 6, 8, 10
 47 U.S.C. § 605 *Communications Act of 1934* 9

Title 50 United States Code, et seq.

50 U.S.C. § 1801 10
 50 U.S.C. § 1804 4, 6
 50 U.S.C. § 1805 10
 50 U.S.C. § 1811 10

Wiretap Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 *passim*

OTHER AUTHORITIES

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>. 14
 Freiwald, Susan, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Alabama L. Rev. 9 (2004) 9, 10, 13

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTEREST OF THE AMICI CURIAE

1
2 Proposed Amici Curiae Law Professors (“Amici”) are law professors whose
3 scholarship, teaching, and practice focus on electronic surveillance and constitutional law.
4 *Amici* wish to highlight for the Court the historical role the judicial branch has played in
5 regulating surveillance and to show that the information necessary to prove or defend against
6 Plaintiffs interception claims is publicly known and not protected by the state secrets
7 privilege.

8 *Amici* are:

9 **Susan Freiwald**
10 Professor of Law
11 UNIVERSITY OF SAN FRANCISCO SCHOOL OF LAW

12 **Cynthia R. Farina**
13 Associate Dean of the University Faculty
14 Professor of Law
15 CORNELL SCHOOL OF LAW

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

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

24 **Erwin Chemerinsky**
25 Alston & Bird Professor of Law and Political Science
26 DUKE UNIVERSITY

27 **SUMMARY OF ARGUMENT**

28 *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

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

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

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

28 ///

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.

1 communication they intercepted. See *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978);
2 *United States v. Councilman* 418 F.3d 67, 84 (1st Cir. 2005). In this case, Defendants’
3 liability under § 2511(1)(a) arises from their interception of Plaintiffs’ communications
4 without a court order. It is irrelevant for purposes of determining Defendants’ liability to
5 whom they provided the communications, or what the recipient did with the information.
6 This Court does not need to know what information, if any, was turned over to the
7 government, or how the government used the information, to find Defendants liable under §
8 2511(1)(a).

9 There is significant evidence before the Court that Defendants intercepted some of
10 their subscribers’ communications. Plaintiffs’ witness Mark Klein describes in his declaration
11 Defendants’ wholesale surveillance of their subscribers’ telephone calls, electronic mail, and
12 internet use. Brief of Amicus Curiae Mark Klein at 4-5. He states that for some subscribers,
13 Defendants’ ongoing practice was to copy the entire flow of the communications traffic to
14 which they had access. *Id.* The activities Klein describes took place on Defendants’ premises
15 and were performed by Defendants’ employees on Defendants’ equipment. The alleged
16 violations occurred at the moment Defendants captured or redirected the contents of the
17 Plaintiffs’ communications. As the Second Circuit has explained, “when the contents of a
18 wire communication are captured or redirected in any way, an interception occurs at that
19 time.” *United States v. Rodriguez*, 968 F.2d at 136. Because an interception occurs at the
20 moment a communication is copied, Plaintiffs need do no more than establish copying to
21 make out a viable claim under 18 U.S.C. § 2511.²

22 Defendants are liable regardless of what they subsequently did with any of the
23 communications they intercepted. See *Jacobson v. Rose*, 592 F.2d at 522. It is irrelevant to
24 Plaintiffs’ interception claims that the National Security Agency (“NSA”) was purportedly the
25

26 ² *Amici* focus on the Wiretap Act and the Electronic Communications Privacy Act rather than
27 FISA because the nature of the plaintiff class, which excludes agents of foreign powers and
28 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).

1 party that received the copies of the intercepted communications and what the NSA might
2 have allegedly done with the communications thereafter. The law asks only if there was an
3 intentional interception of a wire, oral, or electronic communication. For example, in *United*
4 *States v. Councilman*, 418 F.3d 67 (1st Cir. 2005), the defendant, an officer who worked for
5 an electronic communications service provider, made copies of his subscribers' emails in
6 order to learn about his competitor's business practices, and stored those emails in a file on
7 company computers. The First Circuit, *en banc*, held that the defendant violated 18 U.S.C. §
8 2511 because he intercepted his subscribers' communications without either a court order or
9 an applicable exception. Whether or not Councilman subsequently used the communications
10 he obtained was irrelevant to his criminal liability. The violation occurred at the point of
11 unlawful interception. See *Councilman*, 418 F.3d at 84 (“[E]lectronic communications,
12 which are defined expansively, may not be ‘intercepted’.”) (quoting 18 U.S.C. § 2511(1)(a)).
13 Similarly, in this case, it does not matter to the interception claim that the Defendants
14 allegedly forwarded the communications to the NSA. It is the capture of the information
15 itself, not the forwarding, which the statute prohibits.

16 The Government's argument that it would be required to confirm or deny the
17 existence, scope and potential targets of its alleged intelligence activities if this Court were to
18 adjudicate Plaintiffs' claims is therefore in error. The Government's involvement in
19 Defendants' activities, if any, is irrelevant to Plaintiffs' ability to establish that Defendants
20 intercepted Plaintiffs' communications. Plaintiffs, the public, and *amici* are aware that
21 telecommunications carriers like Defendants have both the capability and often the legal
22 responsibility to intercept communications, and that the government often asks them to do so.
23 That is no secret. The issue is whether Defendants did so without authorization here.
24 Defendants could counter Mark Klein's declaration with evidence showing that Defendants
25 did not engage in the particular interceptions alleged in this case. There is no need to disclose
26 state secrets to prove or disprove Plaintiffs' allegations. Therefore, the Court should not
27 dismiss this case as the Government requests.
28

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

3 If Defendants do not dispute Plaintiffs' allegations that they violated 18 U.S.C. §
 4 2511(1)(a), they may defend their actions by establishing that they acted pursuant to a court
 5 order under 18 U.S.C. § 2518.³ In the absence of a valid court order, Defendants may
 6 produce an invalid court order that they relied upon in good faith. *See* 18 U.S.C. § 2520(d).
 7 If Defendants are unable to establish either of these, then they are liable to Plaintiffs for
 8 damages, subject to injunctive relief, and vulnerable to criminal charges. *See* 18 U.S.C. §§
 9 2511(4)(a), 2520. Proving either of these defenses requires the Defendants to produce a court
 10 order. An *in camera* review of that order would not disclose state secrets, and therefore this
 11 case should not be dismissed.

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

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

27 ⁴ The administration has conceded that its domestic surveillance program has operated
 28 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.

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

9 Though the statutory scheme seeks to enforce checks and balances on the executive
 10 branch, the law focuses on the actions of AT&T Corp. and AT&T Inc., not on the actions of
 11 the government. It does not matter whether the government's reason for requesting the
 12 information may implicate state secrets. Defendants still needed to demand a court order, and
 13 whether or not they had one does not implicate state secrets. If Defendants do not rebut the
 14 allegation that they intercepted their subscribers' communications, and if they have no valid
 15 defense, then they should be held liable – as the statute requires. 18 U.S.C. § 2511(1)(a).
 16

17 **II. ESTABLISHED CONSTITUTIONAL AND STATUTORY LAW MANDATE** 18 **JUDICIAL REVIEW OF ELECTRONIC SURVEILLANCE**

19 The Government claims that “no aspect of this case can be litigated without disclosing
 20 state secrets.” Government's Response to Plaintiffs' Memorandum of Points and Authorities,
 21 May 24, 2006, p. 1. The Government's assertion of state secrets is implausibly expansive
 22 given that this Court may consider Plaintiffs' interception claims without divulging state
 23 secrets, as discussed in Part I, *supra*. As to Plaintiffs' other claims, however, *amici* cannot
 24 fully address the Government's assertion, because we have limited access to facts the
 25 Government has presented to the Court.⁵ Nonetheless, the history of electronic surveillance
 26

27 ⁵ Plaintiffs raise claims pertaining to stored communications and communication records, as
 28 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,

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

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

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

21 ///

22 ///

23 ///

24 _____
25 for example, requires proving state action. That requires evidence about the Government’s
26 role in interception that the section 2511 claim does not..

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

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

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

15 Over the next thirty years, government lawyers made other unsuccessful attempts to
16 avoid the law’s restrictions. They argued, for example, that so long as state agents provided
17 them with wiretap-derived information, federal agents could use it in court. The Supreme
18 Court renounced that practice in 1957. See *Benanti v. United States*, 355 U.S. 96, 100 (1957).
19 Although the Court during this period issued decisions that reinforced the federal prohibition
20 against wiretapping, some contemporary commentators saw a reversal of *Olmstead v. United*
21 *States*, 277 U.S. 438 (1928), that would bring Fourth Amendment protection to surveillance
22 targets, as the only way to rein in executive branch surveillance. See Susan Freiwald, *Online*
23 *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).

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

1 used solely to protect national security. The ultimate decision was to permit electronic
2 surveillance only for national security and law enforcement purposes in the Wiretap Act of
3 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212, subject to a comprehensive scheme that
4 carefully circumscribes the use of electronic surveillance by government and private parties
5 alike. *See* Freiwald, 56 Alabama L. Rev. at 13-14, 23-24.⁷

6 Since then, executive branch surveillance has been carefully delimited. For example,
7 when the executive branch advocated the surveillance of domestic threats to national security
8 without a warrant, the Supreme Court rejected that power, although it did not address foreign
9 threats. *See United States v. United States District Court*, 407 U.S. 297 (1972) (“*Keith*”). In
10 1978, Congress enacted the Foreign Intelligence Surveillance Act (“FISA”) in response to
11 reports that the executive branch was abusing its power to conduct foreign intelligence
12 surveillance. *See* 50 U.S.C. §§ 1801-1811. Together, FISA and the Wiretap Act entirely
13 prohibit warrantless electronic surveillance in the United States except for no more than a few
14 days in an emergency, *see* 50 U.S.C. § 1805(f), 18 U.S.C. § 2518(7), and no more than two
15 weeks in the immediate aftermath of the declaration of war. *See* 50 U.S.C. § 1811.

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

26 _____
27 ⁷ Courts have upheld the constitutionality of the Wiretap Act. *See United States v. Donovan*,
28 429 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).

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

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

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

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

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

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

1 intrude on privacy rights.⁸ See, e.g., *United States v. Torres*, 751 F.2d 875, 882-884 (7th Cir.
2 1984); *United States v. Biasucci*, 786 F.2d 504 (2nd Cir. 1986); *United States v. Koyomejian*,
3 970 F.2d 536 (9th Cir.1992) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992).

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

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

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

19 If Plaintiffs' communications were the targets of surveillance that did not meet
20 constitutional and statutory requirements, then the Government may not use the state secrets
21 privilege to conceal those illegal actions. This Court must examine the elements and defenses
22 of each allegation made by Plaintiffs and parse the Government's state secrets claim to
23 determine whether state secrets privileged information is necessary to prove or disprove any
24

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

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

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

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

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

26 ⁹ In its public materials, the Government does not claim that Plaintiffs’ case risks the
27 disruption of diplomatic relations with foreign governments or otherwise impairs the nation’s
28 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).

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

11 If the Government raises legitimate concerns about particular technological sources
 12 and methods, then an approach similar to that under the Classified Information Procedures
 13 Act ("CIPA"), 18 U.S.C. App. III, § 1 *et seq.*, could permit the court to consider classified
 14 materials *in camera*. In *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001), the court
 15 applied CIPA to learn, *ex parte*, about the operation of a key logger system ("KLS") that FBI
 16 agents had installed to obtain the defendant's passphrases for his encrypted files. The court
 17 determined, from the FBI's *in camera* presentation, attended by persons with top-secret
 18 clearance only, that the KLS does not "intercept" under the definition of that term in the
 19 Wiretap Act.¹⁰ The court provided defense counsel with an unclassified summary of the
 20 technology "sufficient to allow the defense to effectively argue the motion to suppress."
 21 *Scarfo*, 180 F. Supp. 2d at 576. Similar procedures, if needed to protect national security,
 22 could be employed in this case. What is not needed is the blanket dismissal of claims just
 23 because they may implicate classified sources and methods for their resolution. See *Ellsberg*
 24 *v. Mitchell*, *supra* at 57. ("Thus the privilege may not be used to shield any material not
 25 strictly necessary to prevent injury to national security....").
 26

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

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

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

25
 26 ¹¹ The Government appears to claim that a privilege over matters relating to NSA operations
 27 requires dismissal. *Amici* point out that if that privilege alone required dismissal, it would
 28 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.

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

4
5 **CONCLUSION**

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

22 ///

23 ///

24 ///

25 ///

1 Dated: June 16, 2006

Respectfully submitted,

2
3 **By:** /S/ Susan Freiwald
Susan Freiwald, *Pro Hac Vice*
4 Voice: (415) 422-6467
5 Email: freiwald@usfca.edu

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

8 *In Pro Se as Amicus Curiae*

9
10 **By:** /S/ Lauren A. Gelman
11 Lauren A. Gelman
Voice: (650) 724-3358
12 Email: gelman@stanford.edu

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

16 STANFORD LAW SCHOOL
CENTER FOR INTERNET & SOCIETY
17 CYBERLAW CLINIC
Crown Quadrangle
18 559 Nathan Abbott Way
Stanford, California 94305-8610

19 *Attorneys for Intervenor Plaintiffs*
20 *Amici Curiae Law Professors*