ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
tien@eff.org
KURT OPSAHL (191303)
kurt@eff.org
KEVIN S. BANKSTON (217026)
bankston@eff.org
CORYNNE MCSHERRY (221504)
corynne@eff.org
JAMES S. TYRE (083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (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)

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' MEMORANDUM OF POINTS AND AUTHORITIES IN RESPONSE TO COURT'S MAY 17, 2006 MINUTE ORDER

PUBLIC REDACTED VERSION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES, RULES AND REGULATIONS

Page

I. INTRODUCTION

The Court's May 17, 2006, Minute Order directs plaintiffs to file a memorandum addressing:

(1) whether this case can be litigated without deciding the state secrets issue, thereby obviating any need for the court to review the government's classified memorandum and declarations and

(2) whether the state secrets privilege is implicated by plaintiffs' FRCP 30(b)(6) deposition request for information whether AT&T received any certification from the government.

Ex parte review of the government's classified memorandum and declarations. The Court's initial concerns regarding the secret *ex parte* review of classified information are well founded. Four substantial reasons weigh against the Court's *ex parte* review of the classified materials at this time.

First, the government's attempt to have this case decided on the basis of secret evidence and arguments raises substantial due process concerns. While such concerns may not dictate that the Court can never review the classified information, they do militate against a review that precludes all access by plaintiffs' counsel or a review that takes place before the Court has had a full opportunity to review the law circumscribing the state secrets privilege and the non-classified record supporting plaintiffs' claims.

Second, Congress itself has directly spoken to the question of access to classified materials that concern surveillance activity where the legality of the surveillance program is at issue – and it has spoken in favor of ***granting*** access to such information, not *ex parte* secrecy. Specifically, 50 U.S.C. §1806(f) provides that "***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." (emphasis added). If the Court deems it necessary to review the secret evidence for the purpose of determining the legality of the program, then plaintiffs' counsel should be granted access to the information subject to all appropriate safeguards.

Third, the record reveals that plaintiffs' claims indeed can proceed in the absence of the classified materials under any reasoned application of the state secrets privilege. This provides a further and independent basis for declining to review the classified materials at this time.

Finally, review of the classified materials at this time is simply premature. Such review would be appropriate only after two points have been crystallized in this case: (1) the government has made a more particularized showing regarding the classified materials; and (2) the Court has determined the appropriate legal ground rules governing the state secrets privilege that the government would invoke, thereby determining just what is in the public domain and what is not. As to the first of these gating events, the government could have provided a non-conclusory showing in support of its need for secrecy – but as of this date has declined to do so. As to the second, the appropriate legal scope of the state secrets privilege is set for full briefing and for argument on June 23, 2006.

Disclosure of the alleged certifications (if any). Plaintiffs' narrow request for discovery under Fed. R. Civ. P. 30(b)(6), limited to any certification that defendant AT&T Corp. received from the government, far from implicating a state secrets privilege, relates to information specifically contemplated by Title III and Foreign Intelligence Surveillance Act of 1978 ("FISA") to be disclosed "as required by legal process." 18 U.S.C. §2511(2)(a). The government can hardly rely on the state secrets privilege when any certification is statutorily required to be disclosed.

II. THE COURT SHOULD NOT REVIEW THE SECRET EVIDENCE OR ARGUMENTS AT THIS TIME

A. Due Process Disfavors Deciding the Case Based on Secret Evidence or Arguments

The examination of *ex parte* information impinges upon "principles of due process upon which our judicial system depends to resolve disputes fairly and accurately." *Lynn v. Regents of Univ. of Cal.*, 656 F.2d 1337, 1346 (9th Cir. 1981). Indeed, "*ex parte* proceedings are anathema in our system of justice." *Guenther v. Comm'r of Internal Revenue*, 889 F.2d 882, 884 (9th Cir. 1989) ("*Guenther I*"), *appeal after remand*, 939 F.2d 758 (9th Cir. 1991) ("*Guenther II*") (quoting *United States v. Thompson*, 827 F.2d 1254, 1258-59 (9th Cir. 1987)). "Notice and an opportunity to be heard are the hallmarks of procedural due process." *Guenther I*, 889 F.2d at 884. Unless a party can see and respond to evidence submitted against it, the Court's impartiality is jeopardized. *Id*; *Guenther II*, 939 F.2d at 760.

Ex parte proceedings that limit a party's ability to participate in hearings, and to consider or even attempt to refute the government's evidence, violate the very spirit of due process. *Id.* Denial of access to the government's submissions defeats plaintiffs' right to fair consideration – indeed any consideration – of their case. *See Guenther I*, 889 F.2d at 884-85. "Only in light of a 'compelling justification' would *ex parte* communications be tolerated." *Guenther II*, 939 F.3d at 760.

It bears emphasis that this is not a case where a party is providing an *in camera* submission for the purpose of demonstrating the privileged character of that submission (as is common in disputes over attorney-client privileged materials). Rather, the government is seeking dismissal of plaintiffs' case on the basis of secret evidence and argument. In such instances, the longstanding teaching that "fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights" is particularly apt. *See Joint Anti-Fascist Refugee Comm. v. McGrath*, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring).

Our adversarial system is based upon "vigorous and informed argument" which is impossible "without disclosure to the parties of the evidence submitted to the court." *Lynn*, 656 F.2d at 1346. To the extent the Court determines it needs more than what is already before it in the record, the Court should proceed incrementally, examining only the least amount of *ex parte* information when – and if – this becomes absolutely necessary. Presently, it is not necessary. At each step, moreover, the Court should determine independently whether the information must be kept from the plaintiffs.

B. Congress Has Provided for Disclosure of Classified Materials to Litigants Challenging the Legality of Surveillance Programs

Congress has recognized the need for due process in electronic-surveillance cases involving national security and has created statutory mechanisms for that purpose. One such mechanism, 50 U.S.C. §1806(f), speaks directly to the question of the access of a litigant challenging the legality of electronic-surveillance. It reads, in pertinent part:

> 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.; *see also* 50 U.S.C. §1845(f) (similar provision for review of evidence necessary to determine legality of the collection of non-content information through pen registers or trap-and-trace devices). Put simply, this provision is the safety valve for the Court's due process concerns. If the Court determines that a review of the classified materials is needed, then it has the authority to disclose those materials to plaintiffs' counsel to the extent "necessary to make an accurate determination of the legality of the surveillance," subject to whatever safeguards the Court deems necessary.[1] The time for such a review, should it eventually be needed, has yet to come.

If and when the time comes to review classified materials, the Court is charged with making sure that "appropriate security procedures" apply. 50 U.S.C. §1806(f). In cases where the government invokes the state secrets privilege, the Court can use "creativity and care [to] devise procedures which [will] protect the privilege and yet allow the merits of the controversy to be decided in some form." *DTM Research, L.L.C. v. AT&T Corp.*, 245 F.3d 327, 334 (4th Cir. 2001) (internal citations omitted). Should the Court determine that it ***must*** review the classified materials urged upon it by the government, the Court should do so under conditions that provide for some form of appropriate access by plaintiffs' counsel.

---

[1] As the Conference Report on 50 U.S.C. §1806(f) explained, "[t]he 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. 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." Foreign Intelligence Surveillance Act of 1978, House Conference Report No. 95-1720, Oct. 5, 1978.

C. The Court Need Not Review the *Ex Parte, In Camera* Material Because Plaintiffs Can Make Their Case Based on the Public Record

1. Plaintiffs Can Sustain Their *Prima Facie* Case Without Resort to the Classified Materials

a. The Key Legal Elements of Plaintiffs' Claims

A review of certain representative claims – the FISA electronic-surveillance and Title III interception claims – shows that plaintiffs can prove their case without relying on privileged information.[2] Title III prohibits the intentional interception of wire and electronic communications. 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). "[C]ontents" include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. §2510(8); *see also* 50 U.S.C. §1801(n) (broader definition for "content" in context of electronic surveillance).

Defendants are "intercepting" those communications under Title III if they acquire copies via the [redacted] described in the declarations plaintiffs have submitted in support of the motion for preliminary injunction. "[W]hen 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 130, 136 (2d Cir. 1992). The same analysis applies to plaintiffs' electronic communications. *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.").

So long as AT&T intercepted class members' communications, plaintiffs need not show the exact method by which the interception was performed, or the exact arrangement between the government and AT&T regarding control of those facilities, for "[Title III's] application should not turn on the type of equipment that is used, but whether the privacy of [communications] has been

---

[2] Plaintiffs have alleged other statutory and constitutional violations, which plaintiffs will also be able to litigate without relying on information subject to the state secrets privilege, as will be explained in detail in plaintiffs' oppositions to the motions to dismiss.

invaded in a manner offensive to the words and intent of the Act." *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979).

Thus, to prevail on their Title III interception claim, plaintiffs need prove only that the communications were unlawfully intercepted.[3] Plaintiffs need not prove what the government did with them. *See Jacobsen v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) ("Because Nevada Bell joined with the Washoe officials in the wiretapping, its failure to listen to the tapes should not insulate it from liability for the invasion of privacy it helped to occasion."). Likewise, to prevail on their claims against AT&T for unlawfully divulging content and non-content records (*i.e.*, call detail records) to the government, plaintiffs simply need prove AT&T has divulged information, not what the government subsequently did with it. *See* 18 U.S.C. §§2511(1)(c), (1)(d), and (3)(a); 47 U.S.C. §605; 18 U.S.C. §2702. As a result, plaintiffs' claims do not require, for example, proof of any specific details about whether or how the government selects particular communications or records to review ***after*** AT&T has unlawfully intercepted or disclosed all of them, or the names or other identifying details of suspects, disclosure of which might arguably harm national security. Such information is simply beside the point.

b. The Factual Bases for Plaintiffs' Claims

The facts needed to prove a violation of Title III are contained within the documents submitted to the Court in support of the motion for preliminary injunction, including the Declaration of Mark Klein and exhibits thereto, or are already within the public domain.[4]

Plaintiffs' already have submitted to the Court evidence of facts showing the violation of Title III. These facts come from Mark Klein's personal knowledge and the analysis of documents

---

[3] FISA defines "electronic surveillance" more broadly, including, among other things, the electronic acquisition, within the United States, of the content of communications to or from the United States or of communications of a "United States person" located in the United States. 50 U.S.C. §1801(f)(n). Common predicate facts would prove plaintiffs' allegations of FISA violations as well as the Title III interception claims.

[4] "Declaration of Mark Klein" or "Klein Decl." refers to the Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction, filed on April 5, 2006.

the Department of Justice has already recognized are not classified. *See* RJN, Exs. D, E.[5] The facts in the record already include the following:

- [redacted]
- [redacted]

From the public statements by government officials, it already is known that, beginning on October 6, 2001, shortly after the September 11, 2001 terrorist attacks, the President directed the NSA to conduct warrantless surveillance of international telephone and Internet communications. The Directors of National Intelligence and the NSA have admitted in a public declaration to this Court that this surveillance program covers "one-end foreign," and thus by implication one-end domestic, communications.[7] Declaration of John D. Negroponte, Director of National Intelligence ("Negroponte Decl."), at 5; Declaration of Lieutenant General Keith B. Alexander, Director, National Security Agency ("Alexander Decl."), at 3. The President has admitted that calls have been intercepted. RJN at 2. The governmental admissions to date thus show that the NSA is conducting surveillance that requires some form of oversight and authorization, whether through a warrant or through the procedures of 18 U.S.C. §2511(2)(a)(ii)(B).

---

[5] "RJN" refers to Plaintiffs' Request for Judicial Notice, filed on March 31, 2006, in support of plaintiffs' Motion for Preliminary Injunction.

[6] "Marcus Decl." refers to the Declaration of J. Scott Marcus in Support of Plaintiffs' Motion for Preliminary Injunction, filed on April 5, 2006.

[7] Although the government's admissions thus far have been limited to its program to intercept international communications, it has failed to deny 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.

United States Attorney General Alberto Gonzales has stated that he believes no warrant or other judicial oversight is required for the surveillance. RJN at 6. General Michael Hayden, the NSA head when the surveillance program began, and Attorney General Gonzales have admitted that the only person who exercises judgment over whether surveillance is reasonable is a "shift supervisor" or "career professional." RJN at 9. General Hayden also admits that the surveillance program is "more aggressive" than what is permissible under FISA, and he admits using it in lieu of FISA procedures. RJN at 7.

2. Adjudication of the Certification Defense Does Not Require Review of the Classified Materials

The government and the AT&T defendants contend that the electronic-surveillance activity at issue in this case may well have been within the law because it was possibly subject to a certification as provided by statute. The governmental admissions to date, however, 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 remaining question, therefore, is whether there has been extra-judicial authorization that satisfies §2511(2)(a)(ii)(B). This fact, however, cannot be immunized from disclosure on the ground of the "state secrets privilege" or because it is adverted to in a classified declaration.

As plaintiffs will more fully brief in their opposition to the government's motion to dismiss, the existence (or non-existence) of a certification cannot constitute a state secret given the very statutory scheme that governs such certifications. Thus, in a passage of the statute omitted from the government's brief on the state secrets privilege, 18 U.S.C. §2511(2)(a)(ii)(B) states that:

> No provider of wire or electronic communication service . . . 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.

Id. (emphasis added).

Thus Title III specifically allows for the disclosure of this information as "***required by the legal process***." *Id.* Put otherwise, if the AT&T defendants are claiming that they have a certification defense, then "legal process" would require the disclosure of the fact of that certification

in the ordinary course of litigation. Nor does the fact that the certification (if it exists) might be included within the classified materials somehow transform it into a "secret." In such circumstances the Court's task was set forth in the *Ellsberg* case: "whenever possible, sensitive information must be disentangled from non sensitive information to allow for the release of the latter." *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983). To the extent the government contends information in such a certification would harm national security if disclosed, the Attorney General may file an affidavit and invoke the procedures of §1806(f), which as discussed above would allow the Court to review – and, as necessary, disclose to plaintiffs – the certification and any other materials related to the surveillance at issue.

Moreover it is doubtful that there is any certification. At least one of AT&T's competitors has acknowledged that the NSA did not offer a certification to answer its concerns about the legality of the eavesdropping program. On May 12, 2006, counsel for the former Chairman and Chief Executive Officer of Qwest, Joe Nacchio, acknowledged that the telecommunications giant had refused to assist the NSA. In his statement, Mr. Nacchio stated that in the fall of 2001, he was approached by the government to permit access to the private telephone records of Qwest's customers. Declaration of Shana E. Scarlett in Support of Plaintiffs' Memorandum of Points and Authorities in Response to Court's May 17, 2006 Minute Order, Ex. 1. Mr. Nacchio stated that he refused such requests because of legal concerns:

> Mr. Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted and that there was a disinclination on the part of the authorities to use any legal process, including the Special Court which had been established to handle such matters, Mr. Nacchio concluded that these requests violated the privacy requirements of the Telecommications Act. Accordingly, Mr. Nacchio issued instructions to refuse to comply with these requests. These requests continued throughout Mr. Nacchio's tenure and until his departure in June of 2002.

Id. Other news articles have similarly reported a lack of certifications provided to telecommunications companies: "Telecommunications executives say MCI, AT&T and Sprint grant the access to their systems without warrants or court orders. Instead, they are cooperating on the basis of oral requests from senior government officials." Declaration of Cindy Cohn in Support of Motion for Preliminary Injunction, Ex. A.

Thus, whether defendants even received a certification by the government remains an open question.

D. Review of the Secret Evidence Is Premature

Due process considerations counsel against review of the classified materials until there is a concrete need to do so. There are two reasons why the Court should defer review of the classified materials proffered by the government:

1. The government has failed to make a particularized showing of the nature of the alleged state secrets and the need to review the classified material; and

2. The Court has yet to define just what falls within the state secrets privilege in this case and what falls outside the privilege – a key predicate in determining whether there is a need to review the classified material.

The need to avoid a premature adjudication of issues pertaining the state secrets privilege, especially one based on materials submitted solely for *ex parte*, *in camera* review, is underscored by the fact that the privilege is an evidentiary doctrine that needs to be applied in the context of concrete disputes over particular documents or statements. The state secrets privilege is a limited evidentiary privilege that "is not to be lightly invoked." *United States v. Reynolds*, 345 U.S. 1, 7 (1953). Although the government seeks to prevent this Court from adjudicating any part of plaintiffs' case, such a wholesale application of the state secrets privilege is unnecessary and inappropriate. *In re United States*, 872 F.2d 472, 478 (D.C. Cir. 1989) (affirming denial of motion to dismiss in favor of "item-by-item determination of privilege"); *Crater Corp. v. Lucent Techs., Inc.*, 423 F.3d 1260, 1267-70 (Fed. Cir. 2005) (reversing order dismissing case where factual record was not sufficiently developed to determine effect of state secrets privilege on plaintiff's claims).

1. The Privilege Should Only Be Applied Once the Government Makes a Particularized Showing Regarding the Alleged State Secrets

Because fundamental due process is at stake, the government must make a more specific showing than it has before this Court may be required to review secret filings *ex parte*. This Court may legitimately demand that more public details be provided, both as to the scope of the claimed state secret or secrets, as well as the claimed potential harm from disclosure:

> The more specific the public explanation, the greater the ability of the opposing party to contest it. The ensuing arguments assist the judge in assessing the risk of harm posed by dissemination of the information in question. This kind of focused debate is of particular aid to the judge when fulfilling his duty to disentangle privileged from non-privileged materials – to ensure that no more is shielded than is necessary to avoid the anticipated injuries.

Ellsberg, 709 F.2d at 63; *see id.* at 64 (noting that in "the case before us . . . considerable time and resources might have been saved by adherence to the principle that *in camera* proceedings should be preceded by as full as possible a public debate over the basis and scope of a privilege claim").

Upholding a district court order enforcing a grand jury subpoena to the President that was intended to permit the court to evaluate presidential executive-privilege claims, the D.C. Circuit in *Nixon v. Sirica*, 487 F.2d 700, 721 (D.C. Cir. 1973) (*en banc*), observed that the proper procedure for assessing claims of executive privilege is to have the President submit, prior to any *in camera* hearing or examination, "more particular claims of privilege, . . . accompanied by an analysis in manageable segments." *Id.* "Without compromising the confidentiality of the information," the D.C. Circuit held, "the analysis should contain descriptions specific enough to identify the basis of the particular claim or claims." *Id.*

Such specificity can, and should, be provided when the government seeks to invoke the state secrets privilege. In *Kasza v. Browner*, 133 F.3d 1159 (9th Cir. 1998), the primary case relied upon by the government in its motion for summary judgment, the government publicly filed an unclassified affidavit that listed ten categories of information it said were covered by its state secrets privilege, providing a public explanation of "why certain environmental data is sensitive to the national security." *Id.* at 1181-83 (Appendix) (setting forth government's unclassified affidavit).

But here, the government has said virtually nothing about what kind of information it claims is subject to the state secrets privilege, or how its disclosure might harm national security – thereby depriving plaintiffs of any reasonable opportunity to oppose the government's arguments. For example, in its motion to dismiss, the government entirely redacts any description of the "categories

of privileged information at issue in this case" and any discussion of why further litigation would inevitably risk the disclosure of state secrets. *See* Gov't Mem. at 13, 16.[8]

Likewise, both the Negroponte and Alexander declarations fail to provide plaintiffs with any specificity about either the kind of information being withheld or how the disclosure would harm national security. For example, Mr. Negroponte states that to discuss the government's surveillance in any greater detail, "would disclose classified intelligence information and reveal intelligence sources and methods." Negroponte Decl., at 5:12-13. The Alexander declaration echoes that information being withheld is "intelligence information, sources, and methods." Alexander Decl., 4:7-8.

The government's discussion of possible harms is no more enlightening. Mr. Negroponte's discussion of the harm to national security is limited to the conclusion that any disclosure "would enable adversaries of the United States to avoid detection by the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of damage to the United States' national security interests." Negroponte Decl., at 5:13-15. Lt. Gen. Alexander states only that disclosure "would severely undermine surveillance activities in general." Alexander Decl., at 4:7-8.

The government has failed to provided plaintiffs and this Court with any indication as to what kind of information relevant to this case is being withheld, or any description of the possible harms that might result from the disclosure. For example, the government does not state whether it contends any certifications received by AT&T are state secrets and what possible harm could result from their disclosure. Likewise, the government does not suggest or claim that the fact of the mass interception of communications itself is a state secret, or what harm could result from the disclosure of this fact. Neither has the government suggested that the fact of AT&T's providing the government with access to call detail records is a state secret, or the harm which would follow from

---

[8] "Motion to Dismiss" or "Gov't Mem" refers to the Memorandum of the United States in Support of the Military and State Secrets Privilege and Motion to Dismiss or, in the Alternative, for Summary Judgment, filed on May 13, 2006.

disclosing this fact. Because plaintiffs' case, as an initial matter, does not rest upon details of how the government utilizes the results of AT&T's mass interception of communications and wholesale disclosure of communications records, the mere fact of the occurrence of such mass interception and disclosure will not reveal state secrets concerning how the government conducts its foreign intelligence investigations.

The government should be required to provide a more specific public explanation of its state secrets claims – such that plaintiffs have an opportunity to answer and rebut its assertions – before this Court can fairly evaluate whether an *ex parte, in camera* review of the government's secret filings might really be needed.

2. A Full Determination of Whether Alleged Secrets Are Implicated Can Only Be Made Following a Determination of What Information Properly Falls Within and Without the State secrets Privilege

The parties disagree about the scope of the state secrets privilege both as a matter of general principle and as it is applied to this case. These disputes are the subject of the briefing that the plaintiffs will submit on June 8, 2006, and of the argument that the Court has set for June 23, 2006. Until those disputes are resolved, it is premature for the Court to determine whether there is a need to review the classified materials in this case for the simple reason that it is not possible to determine what falls within and what falls outside the state secrets privilege in the first instance.

A simple example makes the point. Plaintiffs contend that the existence of the electronic-surveillance program is in the public domain and, therefore, that there is no need to review the government's classified *ex parte* materials that purport to show that this program is subject to the state secrets privilege. If plaintiffs are correct that there is no privilege regarding the existence of the program – whether by virtue of the fact that it has been established by the Klein and Marcus declarations and supporting documents or through public statements of various government officials – this will directly affect the need (or lack thereof) to consider any of the classified information.

Nor does anything that could be set forth within the classified materials affect the determination as to whether material that has already been filed as part of the record in this case constitutes a state secret. Plaintiffs contend that because such material is already in the record in a

non-classified form (even if under seal) it cannot constitute a state secret, regardless of the content of the government's classified materials. Put simply, the government cannot wave a wand over such materials in the form of a classified declaration in a locked briefcase and magically render them a "secret" when they are already in the public square. Perhaps the government disagrees. For present purposes what matters is that until the Court resolves this issue on the merits (an issue set for hearing on June 23, 2006), any consideration of the classified materials is premature.

III. THE STATE SECRET PRIVILEGE DOES NOT BAR DISCOVERY OF ANY CERTIFICATION AT&T MAY HAVE RECEIVED FROM THE GOVERNMENT

As set forth above, §2511(2)(a)(ii) provides for the disclosure of any certifications to the degree that they would ordinarily be called for by "legal process" in this case. Discovery of such certifications is therefore directed by statute.

Plaintiffs' request is neither intrusive or overbroad. Rather, plaintiffs have requested a very limited production of documents related to any certifications received by defendants:

> All Documents that constitute or refer to certifications or purported certifications in writing by a person specified in 18 U.S.C. §2518 (7) or the Attorney General of the United States, as described in 18 U.S.C. §2511(2)(a)(ii)(B), and any other oral or written requests or instructions from the government concerning any interceptions conducted or to be conducted without a court order authorizing such.

Notice of 30(b)(6) Deposition of AT&T Corp., filed May 1, 2006. Plaintiffs are willing to meet and confer to ensure that this request for documents is limited to only those documents necessary to determine the legality of the alleged surveillance. Because this information is properly discoverable evidence and not a state secret as explained above, this evidence should be produced at this time.

If the Court finds that state secrets are implicated, the Court should consider the "appropriate security procedures and protective orders" that could permit plaintiffs access to the information to minimize the infringement on plaintiffs' due process rights. *See, e.g.*, 50 U.S.C. §§1806(f), 1825(g), and 1845(f).

IV. CONCLUSION

For the reasons stated above, plaintiffs respectfully request that the Court decline to review the government's classified memorandum and declarations at this time and grant plaintiffs' request for documents regarding whether AT&T received any certifications from the government.

DATED: May 22, 2006

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN
LEE TIEN
KURT OPSAHL
KEVIN S. BANKSTON
CORYNNE MCSHERRY
JAMES S. TYRE

s/ Lee Tien
LEE TIEN

454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

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

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)

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)

HELLER EHRMAN LLP
ROBERT D. FRAM
MICHAEL M. MARKMAN
333 Bush Street
San Francisco, CA 94104
Telephone: 415/772-6000
415-772-6268 (fax)

Attorneys for Plaintiffs

I, Shana E. Scarlett, am the ECF User whose ID and password are being used to file this PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN RESPONSE TO COURT'S MAY 17, 2006 MINUTE ORDER. In compliance with General Order 45, X.B., I hereby attest that Lee Tien has concurred in this filing.

W:\AT&T Privacy\brf00031130.RED.doc