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' AMENDED NOTICE OF MOTION AND MOTION FOR PRELIMINARY INJUNCTION; PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

[REDACTED]

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Page

Page

Page

CONSTITUTIONS, STATUTES, RULES AND REGULATIONS

Page

SECONDARY AUTHORITIES

TO: ALL PARTIES AND THEIR ATTORNEYS OF RECORD

PLEASE TAKE NOTICE that on June 8, 2006, at 2:00 p.m., in Courtroom 6 of the above-captioned Court, located at 450 Golden Gate Ave., 17th Floor, San Francisco, California, plaintiffs will, and hereby do, move the Court for an order granting preliminary injunctive relief against AT&T Corp. and AT&T Inc. ("defendants").

Plaintiffs seek to preliminarily enjoin defendants from illegally intercepting, disclosing and otherwise using plaintiffs' communications in violation of the Constitution and federal wiretap laws pursuant to Fed. R. Civ. Proc. 65. This motion is based on this notice of motion and motion, memorandum of points and authorities, Plaintiffs' Request for Judicial Notice, the declaration of Cindy Cohn, the declaration of Mark Klein, the declaration of plaintiffs' expert J. Scott Marcus, plaintiffs' motion to extend page limits, plaintiffs' motion to lodge documents under seal (and all associated exhibits and attachments filed herewith), the pleadings and papers on file in this action, discovery to be scheduled and oral arguments of counsel.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs, on behalf of themselves and others similarly situated, request that this Court immediately enter a preliminary injunction enjoining AT&T,[1] the world's largest telecommunications company, from violating the Fourth Amendment of the Constitution and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") by providing the government with direct access to the domestic and international Internet communications of millions of its customers. A preliminary injunction is necessary to prevent irreparable harm to the statutory and constitutional privacy rights of plaintiffs and their fellow AT&T customers until a trial on the merits, where plaintiffs are likely to prove AT&T's continued collaboration with the National Security Agency's illegal and unconstitutional domestic surveillance program.

---

[1] Plaintiffs refer to defendants AT&T Inc. and AT&T Corp. collectively as "AT&T" herein.

The President has publicly admitted that he authorized the National Security Agency ("NSA") to engage in a program of covert, warrantless surveillance of communications of people in the United States, unchecked surveillance that he has declared will continue indefinitely. The NSA did not act alone, however. The evidence provided in support of this motion, along with published statements from members of Congress and numerous and extensive news reports, demonstrate that AT&T has given the NSA direct access to its domestic telecommunications facilities so that it may conduct unfettered dragnet surveillance of private Internet communications transmitted over AT&T's fiber optic network.

AT&T, by providing the government with direct access to the facilities over which its customers' private communications are transmitted, threatens plaintiffs' right to be free from general searches. The Fourth Amendment sprang directly from the Founders' revulsion at the infamous "general warrants" by which the Crown's men randomly rummaged at will through the private papers and possessions of the innocent, *Weeks v. United States*, 232 U.S. 383, 390 (1914), and the "discretionary power given" to "search wherever their suspicions may chance to fall," was rightly rejected as "totally subversive of the liberty of the subject." *Marcus v. Search Warrant of Property*, 367 U.S. 717, 728-29 (1961) (quotation and citation omitted). As the Supreme Court has recognized, electronic surveillance raises the specter of unconstitutional general searches: "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices," *Berger v. New York*, 388 U.S. 41, 63 (1967), because electronic surveillance is "a dragnet . . . [that] intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations." *Id.* at 65 (Douglas, J., concurring).

With this motion, plaintiffs present direct evidence that AT&T has set up a secret, secure room in its [redacted] facility in [redacted] ("[redacted] Facility") – a room to which the NSA regulates access, and into which AT&T has routed its customers' domestic and international Internet communications *en masse*. This room contains sophisticated computer equipment capable of collecting and analyzing the content of all of those millions of communications. The equipment in the secure room is connected to a private communications network, through which the results of its analysis are likely transmitted to the government, and through which the government likely

transmits computerized instructions to the surveillance equipment. The secret room in [redacted] is only the tip of the iceberg, however; the evidence also supports the conclusion that the [redacted] Facility is one of many such NSA-controlled rooms in AT&T facilities across the country. By these actions, AT&T has delivered to the NSA the means to conduct unconstitutional and illegal "dragnet" electronic surveillance of the private communications of AT&T customers, in wholesale violation of law.

Plaintiffs are AT&T customers, and they seek a preliminary injunction to stop AT&T from providing their private communications to the government for its computerized fishing expedition into Americans' private Internet speech.

II. STATEMENT OF FACTS

A. The Government's Statements About the Warrantless Domestic Surveillance Program

Shortly after the September 11, 2001 terrorist attacks, the President authorized the NSA to conduct warrantless surveillance of telephone and Internet communications of persons within the United States. Request for Judicial Notice ("RJN") at ¶¶1, 2; *see also* Declaration of Cindy Cohn ("Cohn Decl."), Exs. C and J (James Risen and Eric Lichtblau, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. Times (Dec. 24, 2005) and James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005)).[2] The President has reauthorized this

---

[2] While newspaper accounts are hearsay, it is well established that this Court has the discretion to consider hearsay or otherwise inadmissible evidence for purposes of deciding whether to issue the preliminary injunction. *Republic of the Philippines v. Marcos*, 862 F.2d 1355, 1363 (9th Cir. 1988) (en banc) (allowing hearsay evidence); *accord Flynt Distrib. Co. v. Harvey*, 734 F.2d 1389, 1394 (9th Cir. 1984) ("The urgency of obtaining a preliminary injunction necessitates a prompt determination and makes it difficult to obtain affidavits from persons who would be competent to testify at trial. The trial court may give even inadmissible evidence some weight, when to do so serves the purpose of preventing irreparable harm before trial."); *Rosen Entm't Sys. LP v. Eiger Vision*, 343 F. Supp. 2d 908 (C.D. Cal. 2004) ("District courts have discretion to consider otherwise inadmissible evidence in ruling on the merits of an application for a preliminary injunction."); *New.Net, Inc. v. Lavasoft*, 356 F. Supp. 2d 1071, 1076 n.3 (C.D. Cal. 2003) ("the Court may, in its discretion, accept hearsay for purposes of deciding whether to issue the preliminary injunction.").

Accordingly, "[d]istrict courts must exercise their discretion in 'weighing all the attendant factors, including the need for expedition,' to assess whether, and to what extent, affidavits or other hearsay materials are 'appropriate given the character and objectives of the injunctive proceeding.'" *Kos Pharm., Inc. v. Andrx Corp.*, 369 F.3d 700 (3d Cir. 2004) (quoting *Asseo v. Pan Am. Grain Co.*,

warrantless surveillance more than thirty times and intends to continue doing so indefinitely. RJN at ¶3.

The government has candidly admitted that the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§1801 *et. seq.*, the statute regulating electronic surveillance for foreign intelligence purposes, "requires a court order before engaging in this kind of surveillance . . . unless otherwise authorized by statute or by Congress." RJN at ¶4. The NSA surveillance program ("Program") admittedly operates "in lieu of" court orders or other judicial authorization, RJN at ¶¶6-7, and neither the President nor Attorney General authorizes the specific interceptions. RJN at ¶9. As General Hayden, Principal Deputy Director for National Intelligence, put it, the Program "is a more . . . 'aggressive' program than would be traditionally available under FISA," in part because "[t]he trigger is quicker and a bit softer than it is for a FISA warrant." RJN at ¶10. The only review process is authorization by an NSA "shift supervisor" for interception of particular individuals' communication. RJN at ¶9.

Administration officials have said that the NSA intercepts communications when the agency has, in its own judgment, a "reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda," as well as the communications of individuals it deems suspicious on the basis of its belief that they have some unspecified "link" to al Qaeda or a related terrorist organization or simply "want to kill Americans." RJN at ¶11.

While admitting that warrantless surveillance is occurring and will continue, RJN at ¶3, the President and other officials have carefully limited their discussions to "the Program as described by the President,"[3] and have consistently refused to confirm that the "Program as described by the

---

805 F.2d 23 (1st Cir. 1986) ("The dispositive question is not their classification as hearsay but whether, weighing all the attendant factors, including the need for expedition, this type of evidence was appropriate given the character and objectives of the injunctive proceeding.").

[3] This limitation is used to create a logical tautology. For example, in Attorney General Alberto Gonzales' February 28, 2006 letter to Senator Arlen Specter, RJN, Attachment 8, he describes the "Terrorist Surveillance Program" as "activities [that] involve the interception by the NSA of the contents of communications in which one party is outside the United States where there

President" constitutes the entirety of the warrantless surveillance that they have been conducting and will continue to conduct. RJN at ¶13. The government is unable to state that the Program includes only limited interceptions of al Qaeda-related international communications as described by the President, because the Program also includes the warrantless interception of the communications of millions of ordinary Americans, made possible through the illegal and unconstitutional cooperation and collaboration of AT&T.

B. AT&T's Collaboration with the Government Program

Numerous major newspapers and other reputable accounts have shown that major U.S. telecommunications companies, including AT&T, are assisting the NSA with the Program. *See* Cohn Decl., Exs. A and B (Leslie Cauley and John Diamond, *Telecoms Let NSA Spy on Calls*, USA Today (Feb. 6, 2006) and Dionne Searcey, Shawn Young and Amol Sharma, *Wiretapping Flap Puts Phone Firms Under Fire*, Wall St. J., Feb. 7, 2006, at B3). Government officials have confirmed that "the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications." Cohn Decl., Ex. C (James Risen and Eric Lichtblau, *Spy Agency Mined Vast Data Trove*, *Officials Report*, N.Y. Times (Dec. 24, 2005)). As early as 2001, "the NSA approached U.S. carriers and asked for their cooperation in a 'data-mining' operation, which might eventually cull 'millions' of individual calls and e-mails." Cohn Decl., Ex. D (Shane Harris and Tim Naftali, *Tinker, Tailor, Miner, Spy*: *Why the NSA's Snooping Is Unprecedented In Scale and Scope*, Slate (Jan. 3, 2006)).

> Following President Bush's order, U.S. intelligence officials secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of America's phone calls. The NSA also gained access to the vast majority of American e-mail traffic that flows through the U.S. telecommunications system.

Cohn Decl., Ex. E at 48 (James Risen, *State of War*: *The Secret History of the CIA and the Bush Administration* (Simon & Schuster 2006)). The new presidential order has given the NSA direct

---

are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization," and then limits his previous testimony to this aspect of the Program. This renders his discussions asserting a limited program meaningless, since the scope of the "Terrorist Surveillance Program" is also limited by the same restrictions.

access to those United States-based telecommunications switches through "back doors." Under the authority of the presidential order, a small group of officials at NSA now monitors telecommunications activity through these domestic switches, searching for terrorism-related intelligence. *Id.* at 48-49.

Furthermore, former Senator Bob Graham has said that when he was chair of the Senate Intelligence Committee in October 2002, administration briefers told him that the President had authorized the NSA to tap into the stream of global telecommunications passing through junctions on U.S. territory, allowing the NSA to intercept "conversations that . . . went through a transit facility inside the United States." Cohn Decl., Ex. F (Barton Gellman, Dafna Linzer and Carol D. Leonnig, *Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, Wash. Post, Feb. 5, 2006, at A01.)

The surveillance under the Program is conducted in several stages, with the early stages being "[c]omputer-controlled systems [that] collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States," and the last stage being actual human scrutiny. *Id.* As Homeland Security Secretary Michael Chertoff confirmed in an interview, the Program involves "'data-mining' – collecting vast amounts of international communications data, running it through computers to spot key words and honing in on potential terrorists." Cohn Decl., Ex. G (Morton Kondracke, *NSA Data Mining Is Legal, Necessary, Chertoff Says*, Roll Call Newspaper (January 25, 2006)).

C. AT&T's Creation of a Secure Room to Facilitate the Government Program's Internet Surveillance

AT&T Corp. (now a subsidiary of AT&T Inc.) maintains domestic telecommunications facilities over which millions of Americans' telephone and Internet communications pass every day. Declaration of Mark Klein[4] ("Klein Decl.") ¶7; *see generally* Cohn Decl. Exs. H and I (*The AT&T*

---

[4] Mr. Klein is a former AT&T Corp. employee who retired in May 2004. Klein Decl., ¶¶2-6. During his 22 years of employment at AT&T Corp., he worked as a communications technician and as a computer network associate at various locations. *Id.*, ¶¶2-5. In the period relevant to this motion, he worked at a facility that handled AT&T's WorldNet International Service ("[redacted]

Advantage, First Quarter 2004 and *SBC Investor Briefing*, No. 246, January 31, 2005). These facilities allow for the transmission of interstate or foreign electronic voice and data communications by the aid of wire, fiber optic cable, or other like connection between the point of origin and the point of reception. Klein Decl., ¶7. One of these facilities is located at the [redacted] Facility. *Id.*, ¶4.

Around January 2003, AT&T Corp. designed and implemented a program in collaboration with the NSA to build a surveillance operation at its [redacted] Facility, inside a secret room known as the "[redacted] Room." *Id.*, ¶¶10, 12, 14, 16-18, 25-31, 34-37 and Klein Decl., Exs. A-C; *see also* Declaration of J. Scott Marcus[5] ("Marcus Decl."), ¶2.

AT&T's [redacted] Facility contains a [redacted] Room, where electronic communications carried by AT&T's [redacted] service are directed to or from AT&T's WorldNet Internet customers. Klein Decl., ¶19. The [redacted] Room is designed to process vast amounts of electronic communications traffic [redacted].

By early 2003, AT&T had connected fiber circuits from the WorldNet Internet Room into a [redacted]

Facility"), *id.*, ¶¶8-9, and at the [redacted] Facility which handled AT&T's WorldNet International Service, such as dial-up and DSL Internet service. *Id.*, ¶¶15, 19.

[5] Mr. Marcus's qualifications are described in his expert declaration and his resume is attached as Exhibit A to that declaration. He has years of experience in designing modern telecommunications networks and served as senior technical advisor for Internet technology to the Federal Communications Commission ("FCC") from July 2001 until July 2005. Prior to his service at the FCC, he was the chief technology officer for a U.S. telecommunications company, Genuity. Marcus Decl., ¶¶7-29.

[6] "Peering" is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. *See* Marcus Decl., ¶¶96-98.

[7] AT&T's Common Backbone network, like backbone networks generally, is used for the transmission of interstate or foreign communications. An Internet backbone can be thought of as a large ISP, many of whose customers may themselves be smaller ISPs. There is no single network that is ***the Internet***; rather, the Internet backbones collectively form the core of the global Internet. *See* Marcus Decl., nn.5-6.

[8] For a discussion of "splitting" fiber optics, *see* Marcus Decl., ¶¶50-63 and 70-73.

[redacted] (hereafter, the [redacted] will be referred to as the "Surveillance Configuration"). *Id.*, ¶¶22-34. It is likely that similar [redacted] were installed in other cities, including [redacted]. *Id.*, ¶36 and Klein Ex. A at 17 (referencing a configuration in [redacted]). An AT&T employee cleared and approved by the NSA was charged with setting up the [redacted] Room, and access to the room was likewise controlled by those NSA-approved AT&T employees. Klein Decl., ¶¶10, 16-18.

D. The Significance of the Surveillance Configuration

According to plaintiffs' expert J. Scott Marcus, who served as a senior technical advisor for Internet technology to the Federal Communications Commission ("FCC") from July 2001 until July 2005 and as a member of the FCC's Homeland Security Policy Council, the Surveillance Configuration is consistent with the media reports describing telecommunications companies' assistance with the Program, and illustrates an infrastructure built and designed by AT&T Corp. to conduct large-scale covert collection and intensive analysis of substantial amounts of both international and domestic Internet communications carried by AT&T Corp.'s network, including domestic communications of AT&T WorldNet Internet service customers such as the plaintiffs. *See* Marcus Decl., ¶¶37-49.

In particular, the position or location of the fiber split in the Surveillance Configuration was not designed to capture only international traffic, and would include purely domestic communications of AT&T customers. *Id.*, ¶¶107-11. A substantial amount of AT&T Corp.'s [redacted] traffic [redacted], was acquired by the Surveillance Configuration, including nearly all of the [redacted] international communications carried at the [redacted] Facility, and a substantial amount of domestic Internet traffic. *Id.*, ¶¶47-49; 91-111.

Furthermore, the Surveillance Configuration includes [redacted], which is designed to analyze large volumes of communications at high speed, and can be programmed to analyze the contents and traffic patterns of the communications acquired by the Surveillance Configuration according to user-defined rules. *Id.*, ¶¶75, 78-85.

The Surveillance Configuration was also connected to an [redacted] from AT&T's Common Backbone, apparently operating at very fast speeds (OC Mps).[9] *Id.*, ¶¶76-77, 86-87. Because NSA regulated physical access to the room, 18, it is reasonable to infer that the government can send and receive data [redacted] to and from the Surveillance Configuration, Marcus Decl., ¶¶76-77, *i.e.*, is the government's "back door." This additional, parallel backbone network wou if AT&T Corp. were merely using the Surveillance Configuration for ordinary b because such analytical results could, and logically would, be transmitted o Backbone. *Id.*, ¶¶76-77, 86-89.

Finally, the evidence indicates that AT&T implemented Surveillance numerous other cities in addition to [redacted]. *Id.*, ¶¶113-18; Klein Decl A fully deployed set of Surveillance Configurations would capture a substantial well over half, of AT&T's purely domestic traffic, representing substantially all o [redacted], which comprises about 10% of all purely communications in the United States. Marcus Decl., ¶¶119-26.

Accordingly, the Klein Declaration and exhibits attached thereto, the Marc the numerous news media accounts show that AT&T has built the capability nec large-scale covert surveillance of electronic communications, and is providing th access to this capability as part of its ongoing and illegal collaboration with warrantless surveillance program.[10]

---

[9] Mps stands for megabits per second. At 155 Mps, one could transfer 10 information contained in a yard of books on a typical bookshelf) in about five se

[10] Plaintiffs are also seeking targeted, early discovery to further confirm, bu these facts. For example, plaintiffs will seek to determine the locations of [redacted]. In addition, the placement [redacted]) suggests that discovery may reveal that AT&T is di telecommunications traffic into the room, including ordinary voice telephone ca

E. The Surveillance Configuration Violates the Rights of Plaintiff Jewel

Representative Plaintiff Carolyn Jewel, a database administrator, book author and teacher in Petaluma, California, is a subscriber and daily user of AT&T Corp.'s WorldNet dial-up Internet service, and has been since approximately June 2000. Declaration of Carolyn Jewel ("Jewel Decl."), ¶¶1-4. As a [redacted] AT&T WorldNet user, Ms. Jewel's electronic communications are being diverted by the Surveillance Configuration in the [redacted] Facility and subjected to surveillance under the Program. Klein Decl., ¶34; Marcus Decl. ¶¶91-112. Ms. Jewel has an expectation of privacy in her electronic communications, and has had her Internet use – both e-mail and otherwise – chilled by the illegal surveillance Program. Jewel Decl., ¶¶5-10.

III. ARGUMENT

A. Plaintiffs Meet the Legal Standard for Preliminary Injunction

A preliminary injunction is proper upon a showing of either "(1) a combination of probable success and the possibility of irreparable harm, or (2) that serious questions are raised and the balance of hardship tips in its favor." *Prudential Real Estate Affiliates, Inc. v. PPR Realty, Inc.*, 204 F.3d 867, 874 (9th Cir. 2000); *accord Republic of the Philippines v. Marcos*, 862 F.2d 1355, 1362 (9th Cir. 1988) (*en banc*); *Hoopa Valley Tribe v. Christie*, 812 F.2d 1097, 1102 (9th Cir. 1987). "These two formulations represent two points on a sliding scale in which the required degree of irreparable harm increases as the probability of success decreases." *Id.* Furthermore, in deciding whether to grant the injunction, "the court must balance the equities between the parties and give due regard to the public interest." *Idaho Watersheds Project v. Hahn*, 307 F.3d 815, 833 (9th Cir. 2002).

A preliminary injunction is a device for "preventing the irreparable loss of rights before judgment." *Sierra On-Line, Inc. v. Phoenix Software, Inc.*, 739 F.2d 1415, 1422 (9th Cir. 1984) (citation omitted). In determining whether a preliminary injunction is proper, "[t]he district court is not required to make any binding findings of fact; it need only find probabilities that the necessary facts can be proved." *Id.* at 1423. Moreover, "the greater the relative hardship to the moving party, the less probability of success must be shown." *Sun Microsystems, Inc. v. Microsoft Corp.*, 188 F.3d 1115, 1119 (9th Cir. 1999), quoting *Nat'l Ctr. for Immigrants Rights v. INS*, 743 F.2d 1365, 1369 (9th Cir. 1984).

Where the balance of hardships tips sharply in the movant's favor, there need not be a probability of success, but only a "serious question" as to which the movant has "fair chance of success on the merits." *Nat'l Wildlife Fed'n v. Coston*, 773 F.2d 1513, 1517 (9th Cir. 1985). "Serious questions are 'substantial, difficult and doubtful, as to make them a fair ground for litigation and thus for more deliberative investigation.'" *Republic of the Philippines*, 862 F.2d at 1362 (quoting *Hamilton Watch Co. v. Benrus Watch Co*., 206 F.2d 738, 740 (2d Cir. 1953)).

Plaintiffs amply meet the standard for preliminary injunctive relief. The balance of harms tilts sharply in favor of plaintiffs, because AT&T will face no harm if it is merely prohibited from continuing to provide wholesale its customers' communications to the government, while plaintiffs will continue to suffer irreparable injury to their constitutional and statutory privacy rights if AT&T is permitted to continue to do so in violation of federal statutes and the Constitution. Plaintiffs are likely to prove the necessary facts that confirm AT&T's role in the Program, and are likely to succeed on the merits – and certainly raise "serious questions" – as to their legal claims. Further, it is strongly in the public interest to enforce the requirements of the wiretapping statutes and the Constitution, and stop AT&T from assisting with a massive government fishing expedition into the communications of millions of ordinary Americans.

B. Plaintiffs Raise Serious Questions and Have a Reasonable Likelihood of Success on the Merits

The facts above, at the very least, raise a serious question as to whether AT&T, by assisting the NSA in its domestic surveillance program, has violated the federal wiretapping statute and assisted in the violation of plaintiffs' Fourth Amendment rights. Considering that the balance of hardships tips strongly in plaintiffs' favor – AT&T would lose nothing by cutting off the NSA's direct access to the communications on its network, while plaintiffs face an ongoing and irreparable injury to their constitutional and statutory privacy rights –a serious question is all plaintiffs must show in order to obtain preliminary relief.

However, more than raising a serious question, the facts demonstrate a likelihood of success on the merits of their two claims: first, that by conducting the surveillance described above, AT&T is "intercepting" plaintiffs' communications, and using and disclosing them, in violation of 18 U.S.C.

§2511; second, that AT&T is acting as an agent of the government, and is seizing and searching plaintiffs' communications for the government in violation of the Fourth Amendment. In the face of such irreparable injury, plaintiffs, who represent millions of ordinary Americans, are entitled to injunctive relief until the legality of AT&T's actions can be finally adjudicated.

1. The Legal Framework: Wiretapping Under the Fourth Amendment and Under Statute

In 1967, the Supreme Court first held that electronic eavesdropping on private communications by the government was a search and seizure subject to the Fourth Amendment. *Berger*, 388 U.S. at 51-60; *Katz v. United States*, 389 U.S. 347, 352-53 (1967). In *Katz*, the Court held that prior judicial review was required because the "far less reliable procedure of an after-the-event justification" is "too likely to be subtly influenced by the familiar shortcomings of hindsight judgment," and "will leave individuals secure from Fourth Amendment violations only in the discretion of the police." *Id.* at 358-59 (citation and quotation omitted).

In response to *Berger* and *Katz*, Congress enacted Title III, Pub. L. No. 90-351, Tit. III, §§801-04, 82 Stat. 211 (codified as amended at 18 U.S.C. §2510 *et seq.*). *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001). Consistent with those decisions, Title III requires law enforcement officers to obtain a search warrant based on probable cause before intercepting wire, oral, or electronic[11] communications in all but emergency situations. 18 U.S.C. §§2511, 2518; *see also United States v. Turner*, 528 F.2d 143, 158-59 (9th Cir. 1975), *cert. denied sub nom.*, *Lewis v. United States*, 423 U.S. 996 (1975) ("[I]n enacting Title III Congress was aware of the decisions of the Supreme Court in this area and had complied with the standards there set forth.").

However, as Congress' broad intent was to "effectively protect the privacy of . . . communications," Title III is not limited to regulating government surveillance. *Bartnicki*, 532 U.S. at 523-24 (citation and quotation omitted). It also generally prohibits ***any person*** from intercepting

---

[11] Title III was amended to protect electronic communications as well as phone conversations by the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat 1848, codified in pertinent part at 18 U.S.C. §§2510(12), 2511(1)(a), 2510(4); *see Bartnicki*, 532 U.S. at 524 (through ECPA, Congress "enlarged the coverage of Title III to prohibit the interception of 'electronic' as well as oral and wire communications").

private communications, or using or disclosing intercepted communications. *Id.*; 18 U.S.C. §2511. Communications providers themselves are subject to this prohibition, except to the extent their conduct is reasonably necessary to providing their service or protecting their rights and property.[12] 18 U.S.C. §2511(2)(a)(i). By so regulating interceptions by providers, Title III – like its predecessor wiretapping statute, 18 U.S.C. §605 – "recognizes that the integrity of the communications system demands that the public be assured that employees who thus come to know the content of messages will in no way breach the trust which such knowledge imposes on them." *Hodge v. Mountain States Telephone and Telegraph Co.*, 555 F.2d 254, 259 (9th Cir. 1977).

Congress soon discovered in the wake of Watergate that communications companies had violated that trust routinely at the NSA's behest. In 1976, a congressional committee headed by Senator Frank Church found that the NSA had engaged in widespread, warrantless domestic electronic surveillance for about thirty years under a program called "Operation Shamrock." *See* S. Rep. No. 94-755 (Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities), 94th Cong., 2d Sess., Book II at 5-20 (1976); *id.*, Book III at 735 (1976) (NSA "intercepted and disseminated internal communications of American citizens" for decades without judicial or congressional oversight). The Church Committee discovered that this illegal surveillance was carried out by the three major international telegraph companies of the day – RCA Global, ITT World Communications and Western Union International – who secretly gave the NSA copies of millions of international telegrams sent to, from, or simply crossing the United States between August 1945 and May 1975. *Id.* at 740.

The need to closely regulate national security surveillance, made evident by the Church Committee's shocking findings, was bolstered by the Supreme Court's earlier decision in *United States v. United States Dist. Court*, 407 U.S. 297, 322 (1972) ("*Keith*") (holding that Fourth Amendment's warrant requirement applied even to wiretaps intended to protect domestic national

---

[12] This allowance for interceptions by communications providers is limited "to such invasion of the subscriber's privacy as is necessary to protect the telephone company's property." *United States v. Goldstein*, 532 F.2d 1305, 1311 (9th Cir. 1976) (quoting *Bubis v. United States*, 384 F.2d 643, 658 n.5 (9th Cir. 1967)).

security, and suggesting that Congress establish protective procedures specific to such wiretaps). "Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent," and the Court thus held that prior judicial approval was required. *Id.* at 321, 323-24.

Responding to *Keith*, as well as to post-Watergate concerns about the Executive's widespread use of warrantless electronic surveillance as revealed by the Church Committee, Congress enacted the FISA in 1978 to establish a regularized procedure for electronic surveillance in the foreign intelligence and counterintelligence field. *See United States v. Belfield*, 692 F.2d 141, 145 (D.C. Cir. 1982); Pub. L. 95-511, Title I, 92 Stat. 1796 (codified as amended at 50 U.S.C. §1801 *et seq.*). FISA requires that foreign-intelligence surveillance of foreign powers and their agents be conducted with prior judicial approval in almost all circumstances, with a only few carefully delimited exceptions,[13] and provides for civil and criminal penalties when such surveillance is conducted under color of law without a court order. 50 U.S.C. §§1809-10.

Together, Title III and FISA generally require judicial authorization for communications surveillance inside the United States. *See* S. Rep. No. 95-604(I) at 6 (1978), 1978 U.S.C.C.A.N. at 3908 (FISA meant to "spell out that the executive cannot engage in electronic surveillance within the United States without a prior Judicial warrant"). Specifically, FISA's amendments to Title III spelled out – to both the Executive and the telecommunications companies that had aided it in the past – that the procedures of Title III and FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. §2511(2)(f). As shown below, the surveillance being conducted here by AT&T on behalf of the government is inconsistent with those procedures, and with the requirements of the Fourth Amendment.

---

[13] *See* discussion at text pp. 19-21.

2. Defendants' Ongoing Surveillance for the Government Violates Title III

AT&T's surveillance via the Surveillance Configuration is a massive, ongoing interception of plaintiffs' communications in violation of Title III and not authorized by FISA. It must be enjoined. 18 U.S.C. §2520 (authorizing "preliminary relief and other equitable or declaratory relief as may be appropriate").

a. Defendants Are Intercepting and Using Plaintiffs' Communications in Violation of 18 U.S.C. Section 2511

The evidence demonstrates that Internet communications between AT&T WorldNet customers and non-AT&T Internet users that are being transferred over AT&T's fiber optic circuits are also being acquired by the Surveillance Configuration. Marcus Decl., ¶¶47-49, 91-111. Title III generally prohibits the intentional interception of wire and electronic communications. 18 U.S.C. §2511(1)(a); *see id.* at §2510(4) (defining "intercept" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device").[14] As detailed below, Title III prohibits AT&T's unauthorized interception of all communications transferred over its fiber optic circuits.

First, the communications being acquired by the Surveillance Configuration, both voice and non-voice, are "communications" protected by Title III. The non-voice Internet communications being transmitted through AT&T's WorldNet facility [redacted],[15] including all e-mails and web pages transmitted over the Internet, are protected "electronic communications]."[16] *See Konop v.*

---

[14] "Contents" includes "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. §2510(8).

[15] This facility is "an electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" under 18 U.S.C. §2510(12). Marcus Decl., n.26.

[16] An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," but not including "wire communications." 18 U.S.C. §2510(12); *see United States v. Herring*, 993 F.2d 784, 787 (11th Cir. 1993) ("As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire).").

Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002) (website was electronic communication), *cert. denied*, 537 U.S. 1193 (2003); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1076-77 (9th Cir.) (e-mails treated as electronic communications), *cert. denied sub nom.*, *Farey-Jones v. Theofel*, 543 U.S. 813 (2004); *see also United States v. Councilman*, 418 F.3d 67, 72-79 (1st Cir. 2005) (en banc) (e-mail was electronic communication); *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503-04 (2d Cir. 2005) (same).

The remaining Internet communications that are transfers of the human voice, such as communications transmitted using Voice-Over-IP ("VOIP") Internet telephone services, are "wire communications."[17] AT&T is indisputably engaged in providing and operating facilities for interstate and foreign communication, and the voice communications transmitted by aid of fiber optic cables through AT&T's WorldNet facility [redacted] are protected wire communications.[18]

Second, defendants are "intercepting" those communications under Title III by acquiring copies via the Surveillance Configuration. "[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at that time." *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d. Cir. 1992), *cert. denied*, 506 U.S. 847 (1992)). The same analysis applies to plaintiffs' electronic communications. *Konop*, 302 F.3d at 878 (for website, construing "intercept" in light of ordinary meaning, *i.e.*, "to stop, seize, or interrupt in progress or course before arrival") (citation omitted); *see also Councilman*, 418 F.3d at 79-80 (acquisition of e-mails from electronic storage intrinsic to the transmission process constitutes interception).

---

[17] A "wire communication" is "any aural transfer made . . . through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate commerce." 18 U.S.C. §2511(1); *see also* 18 U.S.C. §2511(18) ("'aural transfer' means a transfer containing the human voice. . . .").

[18] In discussion of Title III, later reference to unspecified "communications" includes both wire and electronic communications.

Importantly, this Court may properly conclude that plaintiffs' communications have been and are being intercepted even absent knowledge of the exact operational details of [redacted] that are acquiring plaintiffs' communications, or the exact arrangement between the government and AT&T regarding control of those facilities, because "[Title III's] application should not turn on the type of equipment that is used, but whether the privacy of [communications] has been invaded in a manner offensive to the words and intent of the Act." *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979). Nor does it matter whether any human beings personally read or listen to the acquired communications. *See George v. Carusone*, 849 F. Supp. at 163 (finding an interception even though defendants never listened to the acquired communications); *see also 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.") (citing *White v. Weiss*, 535 F.2d 1067, 1071 (8th Cir. 1976)).

It is also irrelevant exactly how AT&T technicians and government personnel have specifically divided their labor in accomplishing the surveillance; any direct participation would be sufficient. *See White*, 535 F.2d at 1071 (conduct of private detective who personally directed a wife's installation of a phone wiretap to monitor her husband constituted an interception, even though it was the wife who personally hooked up the equipment and monitored the phone conversations).

In short, copies of plaintiffs' communications transmitted via AT&T's facilities, including their contents, are being "seized" and "redirected" as a whole into the Surveillance Configuration via the "[redacted]",[19] and such "automatic routing" of communications constitutes "interception" under Title III. *See Councilman*, 418 F.3d at 84-85.

---

[19] The [redacted] is an "electronic, mechanical or other device" for purposes of the definition of "intercept." 18 U.S.C. §2510(5) ("any device or apparatus which can be used to intercept a wire, oral, or electronic communication").

b. Defendants Are Also Disclosing, Using and Divulging Plaintiffs' Communications in Violation of 18 U.S.C. Section 2511

Title III also prohibits the "use" and disclosure of illegally intercepted communications. 18 U.S.C. §§2511(1)(d),[20] 2511(1)(c).[21]

By providing the government with direct access to plaintiffs' communications via the Surveillance Configuration, Marcus Decl., ¶¶39, 88-89, 137-39, AT&T is disclosing those communications to the government in violation of 18 U.S.C. §2511(1)(c). Additionally, by participating in the operation of the Surveillance Configuration, defendants are "using" the illegally intercepted communications. *See Konop*, 302 F.3d at 880 (applying ordinary dictionary definition of "use": "to put into action or service, avail oneself of, employ") (citation and quotations omitted). Although the exact details of the Surveillance Configuration are unknown, they do not need to be known to conclude that the communications that AT&T is intentionally intercepting and diverting into the [redacted] Room are being processed by the Surveillance Configuration – *i.e.*, "put into service" or "employed" – in some fashion. *See* Marcus Decl., ¶¶38, 44, 64-90.

Finally, defendants' disclosure of the content of plaintiffs' communications violates another Title III provision, which specifically prohibits communications providers from divulging the communications they transmit, regardless of whether the communications were lawfully intercepted:

> [A] person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

18 U.S.C. §2511(3)(a). Defendants provide an "electronic communication service" allowing WorldNet customers to send and receive communications over the Internet. *See* 18 U.S.C.

---

[20] 18 U.S.C. §2511(1)(d) prohibits any person from "us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through [an] interception . . . in violation of this subsection."

[21] 18 U.S.C. §2511(1)(c) prohibits any person from "disclos[ing], or endeavor[ing] to disclose, to any person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through [an] interception . . . in violation of this subsection."

§2510(15); Klein Decl., ¶¶7, 9, 19. By intentionally [redacted], a facility to which the government has direct access, AT&T is violating this prohibition and divulging the contents of those communications to the government.

c. Neither Title III nor FISA Authorizes Defendants' Conduct

While generally prohibiting disclosure to the government, both Title III and FISA do provide carefully circumscribed procedures for when a communications provider such as AT&T is authorized to provide the government with "information, facilities, or technical assistance" necessary to accomplish lawful surveillance. 18 U.S.C. §2511(2)(a)(ii). None of those provisions, however, authorize AT&T's ongoing, wholesale provision of its customers' communications to the government demonstrated here.

By statute, AT&T is only authorized to provide surveillance assistance "to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978," and only when AT&T has been provided with:

> (A) a court order directing such assistance signed by the authorizing judge, or (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law [and] that all statutory requirements have been met.

Id. This provision must be read in conjunction with 18 U.S.C. §2511(f), which provides that the procedures of Title III and FISA shall be "the exclusive means" by which interception and electronic surveillance may be conducted.[22] Congress plainly intended that §2511(2)(a)(ii) only authorize

---

[22] The "exclusive means" cited by the statute also include chapter 121 of Title 18, those ECPA provisions dealing with government access to stored communications and records commonly known as the "Stored Communications Act" (SCA), 18 USC §2701-12. However, the SCA only authorizes the government's access to (and the provider's disclosure of) ***stored*** communications and cannot authorize the surveillance described here. *Id.*; *see also* S. Rep. 99-541, at 18 (1986), 1986 U.S.C.C.A.N. 3555, at 3572 (Chapter 121 added as an "exclusive means" in order "to clarify that nothing in . . . [the] proposed chapter 121 affects existing legal authority for U.S. Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. ***It does not provide authority for the conduct of any intelligence activity***." (emphasis added)).

assistance for surveillance that follows those procedures. S. Rep. No. 604(I), at 49050, 62 (1977), 1978 U.S.C.C.A.N. 3904, at 3951, 3963.

Here, the government has admitted that the Program's surveillance has been conducted without court orders, and has continued for several years. RJN at ¶¶3, 6. Furthermore, no certification allowed by statute could authorize the wholesale, long-term interception of customer communications seen here.[23] Title III and FISA allow warrantless surveillance in only the most limited circumstances, and even under those limited circumstances, a court order is usually required eventually, typically in a matter of hours.

Specifically, there are only four situations where the statutes allow for warrantless wiretapping, none of which apply here:

- 50 U.S.C. §1805(f) of FISA provides that the Attorney General may in emergency situations authorize electronic surveillance, but only if a FISA judge is informed at the time of the Attorney General's authorization, and only if an application for a FISA warrant is made to a FISA judge "as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance." *Id.* The surveillance must end after 72 hours, unless a FISA warrant is obtained. *Id.* Yet, by the government's own admission, FISA warrants are not being sought for Program surveillance, and the government has not utilized this emergency provision in FISA. RJN at ¶¶5-6.
- 18 U.S.C. §2518(7) of Title III similarly allows emergency surveillance without a warrant in the law enforcement context, but only if an application is made for a court order within 48 hours; the surveillance must terminate without one. *Id.* Again, the Program's surveillance is done without warrants, and for much longer than 48 hours.
- 50 U.S.C. §1802 authorizes the Attorney General to approve warrantless surveillance for up to one year, but ***only*** if the electronic surveillance "is solely directed at . . . the

---

[23] AT&T can only disclose the existence of any purported certification in response to legal process, *see* 18 U.S.C. 2511(2)(a)(ii), and plaintiffs intend to seek early discovery on this issue.

acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers," or "the acquisition of technical intelligence . . . from property or premises under the open and exclusive control of a foreign power," where "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party. . . ." *Id.* This authority cannot be used to conduct surveillance on AT&T's network, which carries the communications of U.S. persons and is not exclusively used, nor under the exclusive control, of any foreign power. *See* H.R. Conf. Rep. 95-1720, at 25, 1978 U.S.C.C.A.N. 4048, at 4054 ("The Conferees do not intend . . . to authorize the Attorney General to direct electronic surveillance against a line or channel of communication substantially likely to carry conversations or messages of U.S. persons.").

- Finally, 50 U.S.C. §1811 of FISA authorizes warrantless electronic surveillance in the fifteen days following a declaration of war by Congress. War has not been declared, yet the Program has been ongoing since 2001, RJN at ¶3, and AT&T's mass surveillance via the Surveillance Configuration has been ongoing since at least 2003. Klein Decl., ¶31.

As the nation's oldest and largest telecommunications carrier, AT&T cannot credibly plead ignorance regarding the clear requirements of Title III and FISA, including the inapplicability of their warrantless surveillance procedures. As a result, AT&T cannot reasonably and in good faith rely on a certification for conducting this surveillance when such certification is plainly false and unlawful. *See Jacobson*, 592 F.2d at 522 (The defense in 18 U.S.C. §2520 for good-faith reliance on legal demands such as court orders and certifications may be invoked by a defendant "only if he can demonstrate (1) that he had a subjective good faith belief that he acted legally . . . and (2) that this belief was reasonable.").

Even if AT&T asserts that it is reasonably relying on an invalid certification, a preliminary injunction is proper to prevent ongoing harm to AT&T's customers while the lawfulness and reasonableness of AT&T's reliance is fully litigated. In this circuit, "all wire tapping by the

telephone company is subject to close scrutiny by the courts to ensure that the subscriber is not subjected to an unreasonable and overbroad investigation." *Goldstein*, 532 F.2d at 1311. Subscribers of AT&T's WorldNet Internet service are entitled to the same protection.

3. Defendants' Warrantless Surveillance Violates the Fourth Amendment

While Title III provides the simplest route to a preliminary injunction here, and while this Court need not reach the constitutional issue because plaintiffs have demonstrated serious questions about whether Title III has been violated, AT&T's assistance to the Program also violates the Fourth Amendment, and does so even if Title III is satisfied.

The government has stated that surveillance under the Program is conducted without any judicial authorization, and that NSA shift supervisors decide whom to surveil. RJN at ¶¶4-9. Plaintiffs' evidence shows that AT&T is sweeping enormous amounts of private communications into the [redacted] Room in [redacted] (and likely elsewhere) on behalf of the government. Surveillance under the Program thus occurs without any, much less prior, judicial authorization and lacks particularity, completely flouting basic Fourth Amendment principles and law. In short, the Program's suspicionless dragnet surveillance of communications is the 21st-century version of the long-vilified general searches that the Fourth Amendment was intended to eradicate. *See Berger*, 388 U.S. at 56-60.

a. By Assisting the Program, Defendants Are Acting as Agents of the Government

Because AT&T is acting as the agent of the government here, its actions violate the Fourth Amendment. Where a private party such as AT&T "acts as an 'instrument or agent' of the state in effecting a search or seizure, fourth amendment interests are implicated." *United States. v. Walther*, 652 F.2d 788, 792 (9th Cir. 1981) (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971)). The two critical factors in determining whether the defendants were acting as the "instrument[s] or agent[s]" of the government are: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts instead of furthering his own ends. *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982). Both of these factors are met here.

On these facts, there can be no serious doubt that the government knew of and acquiesced in defendants' design and implementation of the Surveillance Configuration to capture millions of private communications traversing AT&T's backbone network. First, NSA agents personally interviewed and cleared two of defendants' technicians to install equipment in the [redacted], and AT&T controlled access to the room in an effort to prevent ordinary AT&T technicians from entering. *See* Klein Decl., ¶¶10, 14, 16-18.

Second, the available facts indicate not only that the government is highly likely to have access to the communications captured by the Surveillance Configuration, Marcus Decl., ¶¶39, 88-89 but that it is highly unlikely that defendants had any independent reason to implement the Surveillance Configuration. *See* Marcus Decl. ¶¶128-39.

Third, media reports independently indicate that AT&T is among the major U.S. telecommunications companies assisting with the Program. Cohn Decl., Exs. A & B (Leslie Cauley and John Diamond, *Telecoms Let NSA Spy on Calls*, USA Today (Feb. 6, 2006) and Dionne Searcey, Shawn Young and Amol Sharma, *Wiretapping Flap Puts Phone Firms Under Fire*, Wall St. J., Feb. 7, 2006, at B3).

Finally, by building a special room, routing communications into it and assisting in specially clearing their technicians to install equipment into the room, the level of involvement between AT&T and the government here is far more extensive than in the ordinary case where a telephone company or telecommunications carrier merely carries out surveillance authorized by a court. *Compare, e.g., Goldstein*, 532 F.2d at 1311 n.6 (telephone company not state actor) ("This is not a case in which the FBI, by secretly (or even unintentionally but effectively) deputizing the telephone company and its investigator, attempted to avoid the restrictions against wiretapping." (citation and internal quotation marks omitted)).

b. Plaintiffs Have a Reasonable Expectation of Privacy in Their Internet Communications

After *Katz*, the Fourth Amendment "now shields private speech from unreasonable surveillance." *Keith*, 407 U.S. at 313 ("the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth

Amendment safeguards." (footnote omitted)). "[T]he Fourth Amendment protects people, not places." *Katz*, 389 U.S. at 351.

Because Title III provides statutory protection for privacy of electronic communications, few courts have had occasion to apply Fourth Amendment standards to Internet transmissions like e-mail. In *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996), however, the Court of Appeals for the Armed Forces found that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant." *Id.* at 418. While the sender bears the risk that "an employee of the company will read e-mail against company policy . . . this is not the same as the police commanding an individual to intercept the message." *Id.*

Importantly, *Katz* did not frame the protections of the Fourth Amendment strictly in terms of privacy, but also in terms of speech. It recognized that "one is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Katz*, 389 U.S. at 352; *cf. Stanford v. Texas*, 379 U.S. 476, 485 (1965) (Fourth Amendment requirements apply with "most scrupulous exactitude" when speech at issue); *Ex parte Jackson*, 96 U.S. 727, 733 (1878) (Fourth Amendment protects letters from search and bars government from conditioning use of postal service on assent to search).

Today, millions of people send and receive e-mail with their friends and loved ones and use the Internet to manage their private financial transactions and learn about political, religious, cultural and health issues. Plaintiffs are AT&T customers who use its electronic communications services to take advantage of this global marketplace of ideas – to read and learn, and to speak to and associate with others. For example, plaintiff Jewel uses defendants' services to send and receive private correspondence about personal matters, including banking, medical, and family matters. Jewel Decl., ¶5. She also uses her AT&T WorldNet service to correspond with individuals in foreign countries, including England, Germany, and Indonesia. *Id.*, ¶4. She reasonably expected and expects these communications to be private. *Id.*, ¶7. She and the AT&T WorldNet customers she represents are surely entitled to assume that the words they type on a computer keyboard and send

over the Internet will only be read by their correspondents, not broadcast to the world or delivered to government agents, just as they expect privacy in the words they speak into a telephone mouthpiece. To read the Constitution to exclude these communications from Fourth Amendment protections is to deny the vital role that the Internet plays in private communication today.

c. Plaintiffs Are Harmed by Defendants' Participation in the Program

AT&T's participation in the Program clearly violates plaintiffs' reasonable expectation of privacy in their communications. As an agent of the government, AT&T's wholesale copying of vast amounts of communications carried by its WorldNet Internet service through the Surveillance Configuration is itself a search and seizure of those communications subject to the Fourth Amendment's strictures. *Berger*, 388 U.S. at 51 (holding that "'conversation' [i]s within the Fourth Amendment's protections, and . . . the use of electronic devices to capture it [i]s a 'search' within the meaning of the Amendment"); *id.* at 59 (unconstitutional state eavesdropping statute authorized "roving commission to 'seize' any and all conversations").

It should also be clear that the Program, putatively grounded in the government's zeal to protect national security, places speech in great jeopardy. "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression. For the serious hazard of suppression of innocent expression inhered in the discretion confided in the officers authorized to exercise the power." *Marcus*, 367 U.S. at 729.

Thus, the Fourth Amendment harm here includes not only the actual search and seizure of communications, but also the chilling effect on speech from plaintiffs' fear of unauthorized surveillance. "It is characteristic of the freedoms of expression in general that they are vulnerable to gravely damaging yet barely visible encroachments." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963). The danger of unauthorized official surveillance parallels the danger of official censorship, which lies "not merely in the sporadic abuse of power by the censor but the pervasive threat inherent in its very existence." *Thornhill v. Alabama*, 310 U.S. 88, 97 (1940).

For example, plaintiff Jewel is currently deterred in her use of defendants' services precisely because of this fear. Until the Program was revealed, she expected that her use of defendants' services was private and that her communications would not be revealed to the government absent appropriate legal process. Jewel Decl., ¶7. Now, she is wary of how she uses the Internet. As an author, she researches subjects she intends to write about, but she now will not use the Internet to research weapons, arms, and military and paramilitary operations for action novels and futuristic romance novels. *Id*., ¶8. Recently, after receiving e-mail from a Muslim correspondent in Indonesia, she chose not to respond openly to religious questions about Islam or political questions about U.S. foreign policy. *Id*., ¶8. Her self-censorship is a perfect example of how "fear of unauthorized official eavesdropping" may "deter vigorous citizen dissent and discussion of Government action in private conversation." *Keith*, 407 U.S. at 314.

d. The Fourth Amendment Prohibits Dragnet, Suspicionless Searches of the Type Present Here

The Fourth Amendment was specifically adopted to prohibit invasions of privacy by indiscriminate, suspicionless searches of the kind that the English Crown had practiced through its infamous use of "general warrants" and "writs of assistance." "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980). "These warrants . . . often gave the most general discretionary authority." *Marcus*, 367 U.S. at 726. "An even broader form of general warrant was the writ of assistance, which met such vigorous opposition in the American Colonies prior to the Revolution." *Id.* at 729 n.22.

"The central objectionable feature of both warrants was that they provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home." *Steagald v. United States*, 451 U.S. 204, 220 (1981). "Moreover, in addition to authorizing search without limit of place, they had no fixed duration. In effect, complete discretion was given to the executing officials; in the words of James Otis, their use placed 'the liberty of every man in the hands of every petty officer.'" *Marcus*, 367 U.S. at 729 n.22.

The Supreme Court has recognized that "[i]t was in the context of . . . general warrants that the battle for individual liberty and privacy was finally won – in the landmark cases of *Wilkes v. Wood* and *Entick v. Carrington*." *Stanford*, 379 U.S. at 483. In *Entick*:

> [Lord] Camden expressly dismissed the contention that such a warrant could be justified on the grounds that it was "necessary for the ends of government to lodge such a power with a state officer. . . ." He declared that these warrants . . . amounted to a "discretionary power given to [Crown officers] to search wherever their suspicions may chance to fall. If such a power is truly invested in a secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject."

Marcus, 367 U.S. at 728-29.

On these foundations, the Fourth Amendment erected an absolute prohibition to general searches of the private writings and communications of an individual. Thus, it is long and well settled that the Fourth Amendment absolutely prohibits indiscriminate, general searches:

> General warrants, of course, are prohibited by the Fourth Amendment. "[T]he problem [posed by the general warrant] is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings. . . . [The Fourth Amendment addresses the problem] by requiring a "'particular description' of the things to be seized." This requirement "'makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'"

Andresen v. Maryland, 427 U.S. 463, 482 (1976) (citations omitted) (alterations in original). The surveillance described here, an automated "rummaging" through the millions of private communications passing over AT&T's fiber optic network at the discretion of NSA staff, is wholly inconsistent with the Fourth Amendment's clear prohibitions.

e. The Program's Sweeping Dragnet Surveillance Cannot Be Reconciled with the Fourth Amendment

The Fourth Amendment's "basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967). The crucial Fourth Amendment protection against such arbitrariness is prior judicial authorization, based on probable cause, and specifying the scope of the search with particularity. In *Katz*, the Supreme Court explained that "bypassing a neutral determination of the scope of a search leaves individuals secure from Fourth Amendment violations only in the discretion of the police." *Katz*, 389 U.S. at 358-59 (internal quotation and citation omitted); *Keith*, 407 U.S. at

318 ("post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights") (citation omitted).

Accordingly, the government's admission that no judicial authorization has been or will be sought for surveillance under the Program, RJN, ¶¶5-7, is sufficient to render AT&T's assistance in searching and seizing plaintiffs' communications unconstitutional.

In addition to lacking prior judicial authorization, the sweeping, dragnet surveillance at issue here is wholly bereft of the particularity and reliability required by the Fourth Amendment. In *Berger*, the Supreme Court condemned the state eavesdropping statute at issue, even though it required prior judicial approval, precisely because it authorized "indiscriminate use of electronic devices" and "actually permits general searches by electronic devices." 388 U.S. at 58. "The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping," which "[b]y its very nature . . . involves an intrusion on privacy that is broad in scope." *Id*. at 56, 57 (heightened scrutiny triggered when surveillance is undertaken as "a series or a continuous surveillance" rather than as "one limited intrusion.").

Here, the dragnet of the Surveillance Configuration captures countless communications without a sliver of particularity, much less evidence of reliability. When communications are captured wholesale in order to sift out possibly suspicious communications, the search is not particularized with respect to any person or communication surveilled and no showing of reliability has been or can be made.

The surveillance of plaintiffs' communications here is the kind of indiscriminate, suspicionless search condemned throughout the history of the Fourth Amendment. But it is also far worse. General searches in the physical world are visible; the general searches under the Program are invisible to the public and the judiciary. General searches aimed at uncovering crime will ultimately be brought to trial, where defendants can challenge the admissibility of evidence; the general searches under the Program are aimed at further covert surveillance that may never see the light of day, much less a courtroom. We only know about warrantless surveillance when the

government decides to tell us about it, and only as much as it decides to tell us. All of the problems of unaccountable arbitrariness posed by general searches in the physical world are magnified with electronic surveillance of the kind that is occurring here.

C. The Balance of Hardships Tilts Sharply in Favor of Plaintiffs

The balance of hardships tilts decidedly toward the plaintiffs here because plaintiffs face irreparable harm to their constitutional and statutory privacy rights from ongoing dragnet surveillance, and AT&T faces no harm from restoring privacy to its customers. This determination reduces the showing that plaintiffs must make on the merits in order to obtain a preliminary injunction, meaning that plaintiffs need only demonstrate that "serious questions" exist, a test easily met here. "The critical element in determining the test to be applied is the relative hardship to the parties. If the balance of harm tips decidedly toward the plaintiff, then the plaintiff need not show as robust a likelihood of success on the merits as when the balance tips less decidedly." *Benda v. Grand Lodge of the Int'l Ass'n of Machinists*, 584 F.2d 308, 315 (9th Cir. 1978), *cert. denied*, 441 U.S. 937 (1979).

1. The Plaintiffs Face Irreparable Harm

a. Plaintiffs Face Irreparable Harm to Their Constitutional Rights

AT&T, acting on behalf of the government, has intercepted plaintiffs' private communications and searched or enabled the government to search their contents, with neither judicial oversight nor prior judicial scrutiny. As demonstrated above, AT&T's warrantless interceptions of private communications on behalf of the government violate the Fourth Amendment. Indeed, the very purpose of the Fourth Amendment is to prevent unreasonable governmental intrusions into one's privacy. The harm to the individual's privacy "is fully accomplished by the original search without probable cause." *United States v. Calandra*, 414 U.S. 338, 354 (1974). The Fourth Amendment harm of unreasonably intercepting conversations, particularly in the interest of national security, comes at the price of "a dread of subjection to an unchecked surveillance power." *Keith*, 407 U.S. at 313-14.

The Ninth Circuit has repeatedly held that where a constitutional violation is part of a "pattern or policy," the irreparable harm prong of the injunctive relief analysis has been satisfied. *Gomez v. Vernon*, 255 F.3d 1228, 1129-30 (9th Cir. 2001) (injunctive relief necessary in light of past pattern of unconstitutional retaliation); *Easyriders Freedom F.I.G.H.T. v. Hannigan*, 92 F.3d 1486, 1500-1501 (9th Cir. 1996) (government misconduct that "flowed from a policy or plan" justified injunctive relief); *Int'l Molders' and Allied Workers' Local Union No. 164 v. Nelson*, 799 F.2d 547, 551 (9th Cir. 1986) (injunctive relief proper where district court found an "evident systematic policy and practice of fourth amendment violations"); *Conner v. City of Santa Ana*, 897 F.2d 1487, 1493-94 (9th Cir. 1990) (government's prior warrantless entry into private yard justified injunctive relief).

Here, the government has repeatedly stated that it will continue its surveillance program unchanged. RJN, ¶3. A governmental policy or plan that violates the Fourth Amendment and that the government has declared it intends to continue makes substantial and immediate irreparable injury not just a likelihood, but a certainty. As the government's agent in carrying out this policy, AT&T must be enjoined from assisting in its implementation.

b. Irreparable Harm Is Presumed Because AT&T Is Violating Title III

Irreparable harm is presumed for violation of statutes, like Title III, that provide for injunctions. *Silver Sage Partners, Ltd. v. City of Desert Hot Springs*, 251 F.3d 814, 827 (9th Cir. 2001); *Smallwood v. Nat'l Can Co.*, 583 F.2d 419, 420 (9th Cir. 1978) (for Title VII claim, holding that where an "injunction [is] issued in response to a statutory provision . . . irreparable harm is presumed from the fact of the violation of the Act"); *Burlington N. R.R. Co. v. Dep't of Revenue*, 934 F.2d 1064, 1074 (9th Cir. 1991) ("When the evidence shows that the defendants are engaged in, or about to be engaged in, the act or practices prohibited by a statute which provides for injunctive relief to prevent such violations, irreparable harm to the plaintiffs need not be shown.").

Pursuant to Title III, this Court is specifically authorized to provide "such preliminary and other equitable or declaratory relief as may be appropriate." 18 U.S.C. §2520. Injunctive relief is necessary because "invasion of privacy, like injury to reputation, inflicts damage which is both difficult to quantify and impossible to compensate fully with money damages." *Williams v. Poulos*,

801 F. Supp. 867, 874 (D. Me. 1992). Accordingly, irreparable injury is presumed upon plaintiffs' showing, set forth above, that AT&T has violated Title III.

2. AT&T Faces No Harm from a Preliminary Injunction

As discussed above, the plaintiffs face significant and irreparable harm from the continuation of the warrantless eavesdropping program. At the same time, there is little if any hardship to AT&T from an injunction requiring it to stop its illegal diversion of Internet traffic to the NSA. Such an injunction would not cause it to incur any direct expenses, nor would it prevent AT&T from providing any services to its customers. "Enforced inaction" generally does not create a threat of harm to be considered in the preliminary injunction context. *Kootenai Tribe of Idaho v. Veneman*, 313 F.3d 1094, 1125 (9th Cir. 2002) (finding that enforced inaction would not threaten harm to the plaintiffs seeking the injunction). Accordingly, the balance of harm tilts sharply toward plaintiffs.

D. A Preliminary Injunction Serves the Public's Interest

"[A]lthough Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern." *Gelbard v. United States*, 408 U.S. 41, 48 (1972); *see also Williams*, 801 F. Supp. at 874 ("There is [a] strong public interest in protecting the privacy and security of communications in a society so heavily dependent on information."). As the Supreme Court noted:

> The Senate committee report that accompanied Title III underscores the congressional policy: "Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. To assure the privacy of oral and wire communications, Title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers engaged in the investigation or prevention of specified types of serious crimes, and only after authorization of a court order obtained after a showing and finding of probable cause."

Gelbard v. United States, 408 U.S. at 48 (quoting S. Rep. No. 90-1097, at 66 (1968)). Accordingly, the public interest is best served by an injunction prohibiting AT&T's cooperation in any wiretapping and electronic surveillance without the authorization of a court order obtained after a showing and finding of probable cause.

To be clear, plaintiffs do not seek the cessation of AT&T's assistance with lawful surveillance conducted pursuant to the proper statutory requirements and judicial authorization. Rather, the injunctive relief sought would simply forbid the massive divulgence of the communications of millions of AT&T customers to the government, while allowing that appropriate targeted domestic eavesdropping be conducted with appropriate judicial oversight, in accordance with constitutional and statutory requirements.

The government has stated that its domestic eavesdropping program serves the interest of national security. *See*, *e.g.*, RJN, Attachment 1. It has long been recognized that, in national security cases, "the investigative duty of the executive may be stronger," but also that such cases involve "greater jeopardy to constitutionally protected speech." *Keith*, 407 U.S. at 313. The warrant requirements of the Fourth Amendment, and the specific provisions for warrants under FISA and Title III, provide a balance between the investigative duties of the executive and the need to protect the liberties of the public. As the Supreme Court has noted, "[t]he 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.

Where the government has probable cause to believe that the target of surveillance is an agent of a foreign power, AT&T can insist upon a warrant from the FISA court, and the government can provide it. The interest in national security may thus be served, without unnecessarily jeopardizing privacy or protected speech.

Accordingly, the proposed injunctive relief serves the public interests which led to Title III and FISA, as well as assuring the pubic that the courts will preserve and defend their constitutionally guaranteed freedoms of speech and association, and their right to be free from unreasonable searches and seizures. At the same time, our national security interests are preserved by the availability of legal surveillance under FISA and Title III.

IV. AMOUNT OF BOND

Whether to require an injunction bond before issuing a preliminary injunction is within the sound discretion of this Court. Fed. R. Civ. Proc. 65(c); *Barahona-Gomez v. Reno*, 167 F.3d 1228,

1237 (9th Cir. 1999). As discussed above, the balance of hardships is overwhelmingly in favor of plaintiffs, who are facing harm to the fundamental rights guaranteed by the Constitution, while AT&T faces neither harm from stopping compliance with the illegal program, nor risk of monetary loss. Accordingly, a bond is unnecessary because there is "no realistic likelihood of harm to the defendant from enjoining his or her conduct." *Jorgensen v. Cassiday*, 320 F.3d 906, 919 (9th Cir. 2003).

V. CONCLUSION

For the reasons stated above, plaintiffs respectfully request that this Court grant their motion for a preliminary injunction.

DATED: April 5, 2006

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

/s/ CINDY COHN
CINDY COHN

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)

Attorneys for Plaintiffs

DECLARATION OF SERVICE BY HAND-DELIVERY

I, the undersigned, declare:

1. That declarant is and was, at all times herein mentioned, a resident of the United States and employed in the City and County of San Francisco, over the age of 18 years, and not a party to or interested party in the within action; that declarant's business address is 100 Pine Street, Suite 2600, San Francisco, California 94111.

2. That on April 5, 2006, declarant served by Hand-Delivery the PLAINTIFFS' AMENDED NOTICE OF MOTION AND MOTION FOR PRELIMINARY INJUNCTION; PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION to the parties listed on the attached Service List.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 5th day of April, 2006, at San Francisco, California.

MARZENA PONIATOWSKA