[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], separate from AT&T's Common Backbone, apparently operating at very fast speeds (OC-3 speeds or 155 Mps).[9] *Id.*, ¶¶76-77, 86-87. Because NSA regulated physical access to the room, Klein Decl., ¶¶17-18, 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.*, [redacted] is the government's "back door." This additional, parallel backbone network would be unnecessary if AT&T Corp. were merely using the Surveillance Configuration for ordinary business purposes, because such analytical results could, and logically would, be transmitted over the Common Backbone. *Id.*, ¶¶76-77, 86-89.

Finally, the evidence indicates that AT&T implemented Surveillance Configurations in numerous other cities in addition to [redacted]. *Id.*, ¶¶113-18; Klein Decl., ¶36, Exs. A-C. A fully deployed set of Surveillance Configurations would capture a substantial fraction, probably well over half, of AT&T's purely domestic traffic, representing substantially all of the AT&T traffic [redacted], which comprises about 10% of all purely domestic Internet communications in the United States. Marcus Decl., ¶¶119-26.

Accordingly, the Klein Declaration and exhibits attached thereto, the Marcus Declaration and the numerous news media accounts show that AT&T has built the capability necessary to conduct large-scale covert surveillance of electronic communications, and is providing the NSA with direct access to this capability as part of its ongoing and illegal collaboration with the government's warrantless surveillance program.[10]

---

[9] Mps stands for megabits per second. At 155 Mps, one could transfer 100 megabytes (the information contained in a yard of books on a typical bookshelf) in about five seconds.

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

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.