

1 ELECTRONIC FRONTIER FOUNDATION  
 CINDY COHN (145997)  
 2 cindy@eff.org  
 LEE TIEN (148216)  
 3 tien@eff.org  
 KURT OPSAHL (191303)  
 4 kurt@eff.org  
 KEVIN S. BANKSTON (217026)  
 5 bankston@eff.org  
 CORYNNE MCSHERRY (221504)  
 6 corynne@eff.org  
 JAMES S. TYRE (083117)  
 7 jstyre@eff.org  
 454 Shotwell Street  
 8 San Francisco, CA 94110  
 Telephone: 415/436-9333  
 9 415/436-9993 (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)

10 Attorneys for Plaintiffs

11 [Additional counsel appear on signature page.]

12 UNITED STATES DISTRICT COURT  
 13 NORTHERN DISTRICT OF CALIFORNIA  
 14

15 TASH HEPTING, GREGORY HICKS, )  
 CAROLYN JEWEL and ERIK KNUTZEN, on )  
 16 Behalf of Themselves and All Others Similarly )  
 Situated, )  
 17 )  
 Plaintiffs, )  
 18 )  
 vs. )  
 19 )  
 AT&T CORP., et al. )  
 20 )  
 Defendants. )  
 21 )

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

22 [REDACTED]  
23  
24  
25  
26  
27  
28

1 **TABLE OF CONTENTS**

2 **Page**

3 I. INTRODUCTION ..... 1

4 II. STATEMENT OF FACTS..... 3

5 A. The Government’s Statements About the Warrantless Domestic  
6 Surveillance Program ..... 3

7 B. AT&T’s Collaboration with the Government Program..... 5

8 C. AT&T’s Creation of a Secure Room to Facilitate the Government  
9 Program’s Internet Surveillance..... 6

10 D. The Significance of the Surveillance Configuration..... 8

11 E. The Surveillance Configuration Violates the Rights of Plaintiff Jewel ..... 10

12 III. ARGUMENT ..... 10

13 A. Plaintiffs Meet the Legal Standard for Preliminary Injunction ..... 10

14 B. Plaintiffs Raise Serious Questions and Have a Reasonable Likelihood of  
15 Success on the Merits ..... 11

16 1. The Legal Framework: Wiretapping Under the Fourth  
17 Amendment and Under Statute ..... 12

18 2. Defendants’ Ongoing Surveillance for the Government Violates  
19 Title III ..... 15

20 a. Defendants Are Intercepting and Using Plaintiffs’  
21 Communications in Violation of 18 U.S.C. Section 2511 ..... 15

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

25 c. Neither Title III nor FISA Authorizes Defendants’ Conduct ..... 19

26 3. Defendants’ Warrantless Surveillance Violates  
27 the Fourth Amendment ..... 22

28 a. By Assisting the Program, Defendants Are Acting  
as Agents of the Government..... 22

b. Plaintiffs Have a Reasonable Expectation of Privacy in  
Their Internet Communications ..... 23

c. Plaintiffs Are Harmed by Defendants’ Participation in the  
Program ..... 25

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

	<b>Page</b>
d.    The Fourth Amendment Prohibits Dragnet, Suspicionless Searches of the Type Present Here.....	26
e.    The Program’s Sweeping Dragnet Surveillance Cannot Be Reconciled with the Fourth Amendment.....	27
C.    The Balance of Hardships Tilts Sharply in Favor of Plaintiffs.....	29
1.    The Plaintiffs Face Irreparable Harm .....	29
a.    Plaintiffs Face Irreparable Harm to Their Constitutional Rights.....	29
b.    Irreparable Harm Is Presumed Because AT&T Is Violating Title III.....	30
2.    AT&T Faces No Harm from a Preliminary Injunction.....	31
D.    A Preliminary Injunction Serves the Public’s Interest .....	31
IV.    AMOUNT OF BOND.....	32
V.    CONCLUSION .....	33

**TABLE OF AUTHORITIES**

		<b>Page</b>
1		
2		
3	<i>Andresen v. Maryland</i> ,	
4	427 U.S. 463 (1976).....	26
5	<i>Asseo v. Pan Am. Grain Co.</i> ,	
6	805 F.2d 23 (1st Cir. 1986).....	3
7	<i>Bantam Books, Inc. v. Sullivan</i> ,	
8	372 U.S. 58 (1963).....	25
9	<i>Barahona-Gomez v. Reno</i> ,	
10	167 F.3d 1228 (9th Cir. 1999).....	31
11	<i>Bartnicki v. Vopper</i> ,	
12	532 U.S. 514 (2001).....	12
13	<i>Benda v. Grand Lodge of the Int'l Ass'n of Machinists</i> ,	
14	584 F.2d 308 (9th Cir. 1978),	
15	<i>cert. denied</i> , 441 U.S. 937 (1979).....	28
16	<i>Berger v. New York</i> ,	
17	388 U.S. 41 (1967).....	<i>passim</i>
18	<i>Bubis v. United States</i> ,	
19	384 F.2d 643 (9th Cir. 1967).....	13
20	<i>Burlington N. R.R. Co. v. Dep't of Revenue</i> ,	
21	934 F.2d 1064 (9th Cir. 1991).....	29
22	<i>Camara v. Municipal Court</i> ,	
23	387 U.S. 523 (1967).....	26
24	<i>Campiti v. Walonis</i> ,	
25	611 F.2d 387 (1st Cir. 1979).....	17
26	<i>Conner v. City of Santa Ana</i> ,	
27	897 F.2d 1487 (9th Cir. 1990).....	29
28	<i>Coolidge v. New Hampshire</i> ,	
29	403 U.S. 443 (1971).....	22
30	<i>Easyriders Freedom F.I.G.H.T. v. Hannigan</i> ,	
31	92 F.3d 1486 (9th Cir. 1996).....	29
32	<i>Ex parte Jackson</i> ,	
33	96 U.S. 727 (1878).....	24
34	<i>Flynt Distrib. Co. v. Harvey</i> ,	
35	734 F.2d 1389 (9th Cir. 1984).....	3
36	<i>Gelbard v. United States</i> ,	
37	408 U.S. 41 (1972).....	30

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

**Page**

*George v. Carusone*,  
849 F. Supp. 159 (D. Conn. 1994)..... 16, 17

*Gomez v. Vernon*,  
255 F.3d 1228 (9th Cir. 2001)..... 29

*Hall v. EarthLink Network, Inc.*,  
396 F.3d 500 (2d Cir. 2005)..... 16

*Hodge v. Mountain States Telephone and Telegraph Co.*,  
555 F.2d 254 (9th Cir. 1977)..... 13

*Hoopa Valley Tribe v. Christie*,  
812 F.2d 1097 (9th Cir. 1987)..... 10

*Idaho Watersheds Project v. Hahn*,  
307 F.3d 815 (9th Cir. 2002)..... 10

*Int'l Molders' and Allied Workers' Local Union No. 164 v. Nelson*,  
799 F.2d 547 (9th Cir. 1986)..... 29

*Jacobsen v. Rose*,  
592 F.2d 515 (9th Cir. 1978)..... 17, 21

*Jorgensen v. Cassidy*,  
320 F.3d 906 (9th Cir. 2003)..... 32

*Katz v. United States*,  
389 U.S. 347 (1967)..... *passim*

*Konop v. Hawaiian Airlines, Inc.*,  
302 F.3d 868 (9th Cir. 2002),  
*cert. denied*, 537 U.S. 1193 (2003)..... 15, 16, 18

*Kootenai Tribe of Idaho v. Veneman*,  
313 F.3d 1094 (9th Cir. 2002)..... 30

*Kos Pharm., Inc. v. Andrx Corp.*,  
369 F.3d 700 (3d Cir. 2004)..... 3

*Marcus v. Search Warrant of Property*,  
367 U.S. 717 (1961)..... 2, 25, 26

*Nat'l Ctr. for Immigrants Rights v. INS*,  
743 F.2d 1365 (9th Cir. 1984)..... 10

*Nat'l Wildlife Fed'n v. Coston*,  
773 F.2d 1513 (9th Cir. 1985)..... 11

*New.Net, Inc. v. Lavasoft*,  
356 F. Supp. 2d 1071 (C.D. Cal. 2003) ..... 3

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

**Page**

*Payton v. New York*,  
445 U.S. 573 (1980)..... 25

*Prudential Real Estate Affiliates, Inc. v. PPR Realty, Inc.*,  
204 F.3d 867 (9th Cir. 2000)..... 10

*Republic of the Philippines v. Marcos*,  
862 F.2d 1355 (9th Cir. 1988).....3, 10, 11

*Rosen Entm't Sys. LP v. Eiger Vision*,  
343 F. Supp. 2d 908 (C.D. Cal. 2004) ..... 3

*Sierra On-Line, Inc. v. Phoenix Software, Inc.*,  
739 F.2d 1415 (9th Cir. 1984)..... 10

*Silver Sage Partners, Ltd. v. City of Desert Hot Springs*,  
251 F.3d 814 (9th Cir. 2001)..... 29

*Smallwood v. Nat'l Can Co.*,  
583 F.2d 419 (9th Cir. 1978)..... 29

*Stanford v. Texas*,  
379 U.S. 476 (1965).....24, 26

*Steagald v. United States*,  
451 U.S. 204 (1981)..... 25

*Sun Microsystems, Inc. v. Microsoft Corp.*,  
188 F.3d 1115 (9th Cir. 1999)..... 10

*Theofel v. Farey-Jones*,  
359 F.3d 1066 (9th Cir.), cert. denied sub nom.,  
*Farey-Jones v. Theofel*, 543 U.S. 813 (2004) ..... 16

*Thornhill v. Alabama*,  
310 U.S. 88 (1940)..... 25

*United States v. Belfield*,  
692 F.2d 141 (D.C. Cir. 1982)..... 14

*United States v. Calandra*,  
414 U.S. 338 (1974)..... 28

*United States v. Councilman*,  
418 F.3d 67 (1st Cir. 2005) .....16, 17

*United States v. Goldstein*,  
532 F.2d 1305 (9th Cir. 1976)..... 13, 22, 23

*United States v. Herring*,  
993 F.2d 784 (11th Cir. 1993)..... 15

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

**Page**

*United States v. Maxwell*,  
45 M.J. 406 (C.A.A.F. 1996)..... 24

*United States v. Miller*,  
688 F.2d 652 (9th Cir. 1982)..... 22

*United States v. Rodriguez*,  
968 F.2d 130 (2d. Cir. 1992),  
*cert. denied*, 506 U.S. 847 (1992)..... 16

*United States v. Turner*,  
528 F.2d 143 (9th Cir. 1975), *cert. denied sub nom.*,  
*Lewis v. United States*, 423 U.S. 996 (1975)..... 12

*United States v. United States Dist. Court*,  
407 U.S. 297 (1972).....*passim*

*United States v. Walther*,  
652 F.2d 788 (9th Cir. 1981)..... 22

*Weeks v. United States*,  
232 U.S. 383 (1914)..... 2

*White v. Weiss*,  
535 F.2d 1067, 1071 (8th Cir. 1976) ..... 17

*Williams v. Poulos*,  
801 F. Supp. 867 (D. Me. 1992).....29, 30

**CONSTITUTIONS, STATUTES, RULES AND REGULATIONS**

U.S. Const. amend. IV.....*passim*

50 U.S.C.

§1801..... 4

§1802..... 20

§1805(f)..... 20

§§1809-10..... 14

§1811..... 21

18 U.S.C.

§605..... 13

§2510(4) ..... 15, 16, 18

§2510(5) ..... 17

§2510(8) ..... 15

§2510(12) .....*passim*

§2510(15) ..... 18

§2511.....*passim*

§2511(1).....*passim*

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

**Page**

§2511(2) ..... 13  
§2511(3) ..... 18  
§2511(18) ..... 16  
§2511(f) ..... 19  
§2518 ..... 12  
§2518(7) ..... 20  
§2520 ..... 15, 21, 29  
§2701-12 ..... 19

**SECONDARY AUTHORITIES**

H.R. Conf. Rep. 95-1720,  
*as reprinted in* 1978 U.S.C.C.A.N. 4048 ..... 21  
S. Rep. 99-541,  
*as reprinted in* 1986 U.S.C.C.A.N. 3555 ..... 19  
S. Rep. No. 94-755 (1976) ..... 13  
S. Rep. No. 604(I),  
*as reprinted in* 1978 U.S.C.C.A.N. 3904, 3951, 3963 ..... 14, 20



1 TO: ALL PARTIES AND THEIR ATTORNEYS OF RECORD

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

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

14 **MEMORANDUM OF POINTS AND AUTHORITIES**

15 **I. INTRODUCTION**

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

25

26

---

27 <sup>1</sup> Plaintiffs refer to defendants AT&T Inc. and AT&T Corp. collectively as “AT&T” herein.

28

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

9 AT&T, by providing the government with direct access to the facilities over which its  
10 customers’ private communications are transmitted, threatens plaintiffs’ right to be free from general  
11 searches. The Fourth Amendment sprang directly from the Founders’ revulsion at the infamous  
12 “general warrants” by which the Crown’s men randomly rummaged at will through the private  
13 papers and possessions of the innocent, *Weeks v. United States*, 232 U.S. 383, 390 (1914), and the  
14 “discretionary power given” to “search wherever their suspicions may chance to fall,” was rightly  
15 rejected as “totally subversive of the liberty of the subject.” *Marcus v. Search Warrant of Property*,  
16 367 U.S. 717, 728-29 (1961) (quotation and citation omitted). As the Supreme Court has  
17 recognized, electronic surveillance raises the specter of unconstitutional general searches: “[f]ew  
18 threats to liberty exist which are greater than that posed by the use of eavesdropping devices,”  
19 *Berger v. New York*, 388 U.S. 41, 63 (1967), because electronic surveillance is “a dragnet . . . [that]  
20 intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of  
21 conversations.” *Id.* at 65 (Douglas, J., concurring).

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

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

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

## 10 II. STATEMENT OF FACTS

### 11 A. The Government's Statements About the Warrantless Domestic 12 Surveillance Program

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

---

19  
20 <sup>2</sup> While newspaper accounts are hearsay, it is well established that this Court has the discretion  
21 to consider hearsay or otherwise inadmissible evidence for purposes of deciding whether to issue the  
22 preliminary injunction. *Republic of the Philippines v. Marcos*, 862 F.2d 1355, 1363 (9th Cir. 1988)  
23 (en banc) (allowing hearsay evidence); *accord Flynt Distrib. Co. v. Harvey*, 734 F.2d 1389, 1394  
24 (9th Cir. 1984) ("The urgency of obtaining a preliminary injunction necessitates a prompt  
25 determination and makes it difficult to obtain affidavits from persons who would be competent to  
26 testify at trial. The trial court may give even inadmissible evidence some weight, when to do so  
27 serves the purpose of preventing irreparable harm before trial."); *Rosen Entm't Sys. LP v. Eiger*  
28 *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.*,

1 warrantless surveillance more than thirty times and intends to continue doing so indefinitely. RJN at  
2 ¶3.

3 The government has candidly admitted that the Foreign Intelligence Surveillance Act of 1978  
4 (“FISA”), 50 U.S.C. §§1801 *et. seq.*, the statute regulating electronic surveillance for foreign  
5 intelligence purposes, “requires a court order before engaging in this kind of surveillance . . . unless  
6 otherwise authorized by statute or by Congress.” RJN at ¶4. The NSA surveillance program  
7 (“Program”) admittedly operates “in lieu of” court orders or other judicial authorization, RJN at ¶¶6-  
8 7, and neither the President nor Attorney General authorizes the specific interceptions. RJN at ¶9.  
9 As General Hayden, Principal Deputy Director for National Intelligence, put it, the Program “is a  
10 more . . . ‘aggressive’ program than would be traditionally available under FISA,” in part because  
11 “[t]he trigger is quicker and a bit softer than it is for a FISA warrant.” RJN at ¶10. The only review  
12 process is authorization by an NSA “shift supervisor” for interception of particular individuals’  
13 communication. RJN at ¶9.

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

20 While admitting that warrantless surveillance is occurring and will continue, RJN at ¶3, the  
21 President and other officials have carefully limited their discussions to “the Program as described by  
22 the President,”<sup>3</sup> and have consistently refused to confirm that the “Program as described by the  
23

---

24 805 F.2d 23 (1st Cir. 1986) (“The dispositive question is not their classification as hearsay but  
25 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.”).

26 <sup>3</sup> This limitation is used to create a logical tautology. For example, in Attorney General  
27 Alberto Gonzales’ February 28, 2006 letter to Senator Arlen Specter, RJN, Attachment 8, he  
28 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

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

7 **B. AT&T’s Collaboration with the Government Program**

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

20 Following President Bush’s order, U.S. intelligence officials secretly arranged with  
21 top officials of major telecommunications companies to gain access to large  
22 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.

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

25  
26 are reasonable grounds to believe that at least one party to the communication is a member or agent  
27 of al Qaeda or an affiliated terrorist organization,” and then limits his previous testimony to this  
28 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.

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

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

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

20 **C. AT&T’s Creation of a Secure Room to Facilitate the Government**  
21 **Program’s Internet Surveillance**

22 AT&T Corp. (now a subsidiary of AT&T Inc.) maintains domestic telecommunications  
23 facilities over which millions of Americans’ telephone and Internet communications pass every day.  
24 Declaration of Mark Klein<sup>4</sup> (“Klein Decl.”) ¶7; *see generally* Cohn Decl. Exs. H and I (*The AT&T*

25 \_\_\_\_\_  
26 <sup>4</sup> Mr. Klein is a former AT&T Corp. employee who retired in May 2004. Klein Decl., ¶¶2-6.  
27 During his 22 years of employment at AT&T Corp., he worked as a communications technician and  
28 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 (“██████████”).

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

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

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

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

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

20 <sup>5</sup> Mr. Marcus’s qualifications are described in his expert declaration and his resume is attached  
21 as Exhibit A to that declaration. He has years of experience in designing modern  
22 telecommunications networks and served as senior technical advisor for Internet technology to the  
23 Federal Communications Commission (“FCC”) from July 2001 until July 2005. Prior to his service  
24 at the FCC, he was the chief technology officer for a U.S. telecommunications company, Genuity.  
25 Marcus Decl., ¶¶7-29.

26 <sup>6</sup> “Peering” is the process whereby Internet providers interchange traffic destined for their  
27 respective customers, and for customers of their customers. *See* Marcus Decl., ¶¶96-98.

28 <sup>7</sup> 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.

<sup>8</sup> For a discussion of “splitting” fiber optics, *see* Marcus Decl., ¶¶50-63 and 70-73.