Appeal Nos. 06-17132 and 06-17137

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

TASH HEPTING, *et al.*,
Plaintiffs/Appellees,

v.

AT&T CORP.,
Defendant/Appellant.

TASH HEPTING, *et al.*,
Plaintiffs/Appellees,

v.

United States,
Defendant-Intervenor/Appellant.

On Appeal from the United States District Court for the Northern District of California

---

AMICI CURIAE BRIEF OF CONSUMER RIGHTS GROUPS: CENTER FOR DIGITAL DEMOCRACY, CONSUMER FEDERATION OF AMERICA, CONSUMERS UNION, PRIVACYACTIVISM AND U.S. PUBLIC INTEREST RESEARCH GROUP

IN SUPPORT OF APPELLEES

Jennifer Stisa Granick
Lauren Gelman
Shannon Kenealy, Law Student
CYBERLAW CLINIC
STANFORD LAW SCHOOL
Crown Quadrangle
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 724-0014
Facsimile: (650) 723-4426

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

U.S. CONSTITUTION

FEDERAL CASES

FEDERAL STATUTES

PUBLIC LAWS AND BILLS

LEGISLATIVE HISTORY

STATE STATUTES

MISCELLANEOUS

INTEREST OF THE *AMICI CURIAE*

Pursuant to Federal Rule of Appellate Procedure 28, *Amici Curiae* ("*Amici*"), by their undersigned counsel, submit this amicus brief in support of Tash Hepting *et al.*, the class Plaintiffs in the above captioned matter. All parties have consented to the filing of this amicus.

Amici, Center for Digital Democracy, Consumer Federation of America, Consumers Union, PrivacyActivism and the U.S. Public Interest Research Group are consumers and consumer advocacy groups advocating for adequate privacy protections for Americans telephone and email communications.

The Center for Digital Democracy ("CDD") is a nonprofit organization incorporated in the District of Columbia. CDD is committed to preserving the openness and diversity of the Internet in the broadband era, and to realizing the full potential of digital communications through the development and encouragement of noncommercial, public interest programming. CDD has recently filed with the Federal Trade Commission a Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices in addition to a Complaint and Request for Inquiry into the recent merger between Google and DoubleClick.

The Consumer Federation of America ("CFA") is an advocacy, research, education, and service organization that consists of some 300 nonprofit organizations from throughout the nation with a combined membership exceeding 50 million people—enabling CFA to speak for virtually all consumers. By gathering facts, analyzing issues, and disseminating information to the consumers and policymakers, CFA provides consumers with a voice in decisions that affect their lives.

Consumers Union ("CU") is an expert, independent, nonprofit organization, whose mission is to work for a fair, just, and safe marketplace for all consumers. CU publishes Consumer Reports and ConsumerReports.org in addition to two newsletters, Consumer Reports on Health and Consumer Reports Money Adviser with combined subscriptions of more than 7 million. Consumers Union also has nearly 400,000 online activists who help work to change legislation and the marketplace in favor of the consumer interest and several public education Web sites.

PrivacyActivism is a nonprofit organization that endeavors to inform consumers about the importance of privacy in the era of electronic information exchange. Digital technology often makes the concept of personal privacy seem

too abstract to grasp. PrivacyActivism tries to make clear the consequences of choices consumers make every day about revealing their information in order to increase the public's understanding of the steady erosion of personal privacy and the importance of conserving it.

The U.S. Public Interest Research Group ("U.S. PIRG"), incorporated in Washington, DC, serves as both the federal advocacy office for and the federation of nonprofit, non-partisan state Public Interest Research Groups, with over one million members nationwide. U.S. PIRG is a strong supporter of fair, competitive marketplace practices, including compliance with the OECD Guidelines for the Protection of Privacy.

INTRODUCTION

Plaintiffs allege that AT&T is collaborating with the National Security Agency (NSA) in a massive warrantless surveillance program that illegally tracks the domestic and foreign communications and communication records of millions of Americans. Plaintiffs allege that AT&T's actions violate the First and Fourth Amendments to the United States Constitution, the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 USC 1809, the Electronic Communications Privacy Act (ECPA), 18 USC 2511(1)(a), (1)(c), (1)(d) and (3)(a), the

Communications Act of 1934, 47 USC 605, the Stored Communications Act (SCA), 18 USC 2702(a)(1), (a)(2), 2702(a)(3) and California's Unfair Competition Law, Cal Bus & Prof Code 17200 *et seq*. The United States moved to intervene in the case, and both the government and AT&T have moved to dismiss on the grounds that litigating this case would impermissibly reveal state secrets. U.S. District Court Judge Vaughn Walker denied the Motions to Dismiss, and AT&T and the government appealed.

If the allegations in this lawsuit are true, consumers have been betrayed by defendant AT&T's unlawful surveillance of their private communications. Defendant and its *amici* United States Telecom Association and the U.S. Chamber of Commerce argue that even if AT&T conducted illegal surveillance, the case is not and should not be litigable, because AT&T did so in secret collusion with the government. Courts should view secret agreements between government and industry, especially ones that abrogate fundamental constitutional rights of Americans, with great alarm rather than deference. Secrecy engenders abuse. Therefore, *Amici* urge this Court to allow this litigation to go forward. Neither the Constitution, Title III (The Wiretap Act of 1968 as amended by ECPA and later statutes), nor FISA tolerates secret illegal relationships between communications providers and the Executive Branch. Dismissal of this case would leave consumers without protection for their privacy from unlawful and unwarranted intrusion.

Communications service providers like AT&T play an indispensable role in preventing illegal interception and disclosure. Consumers may have no idea when their calls and emails are monitored. While both the Constitution and federal law require close judicial supervision of communications surveillance, courts are poorly situated to ensure that the surveillance they authorize is properly conducted. Because surveillance takes place at the service providers' facilities, only providers are in the position to ensure that law enforcement acts legally. In short, service providers are a crucial second line of defense for consumers. By imposing civil liability on service providers who intercept communications without a valid court order, Congress ensured that service providers would be guardians of constitutionally- and statutorily-protected communications privacy. Dismissing cases like this would mean that no one would serve this fiduciary role and leaves customers open to overreaching and abuse.

There is no doubt that national security often depends on government cooperation with businesses. But that cooperation must be **legal**. The Manhattan Project, the manufacture of armaments for war-making, and other collaboration between business and government that *Amici* U.S. Telecom and the Chamber of Commerce extol are all legal powers of the Executive Branch, unregulated by the Bill of Rights. Dismissing the case at this point means that government may conduct secret surveillance programs that never face judicial scrutiny that ensures

consumers' privacy rights have not been unduly trampled upon. We therefore respectfully urge the Court to affirm the District Court's order denying AT&T's and the government's motions to dismiss the Plaintiffs' claims.

I. CONGRESS IMPOSED CIVIL LIABILITY ON SERVICE PROVIDERS TO ENSURE THEY WOULD ACT AS GUARDIANS OF CUSTOMER PRIVACY AND PROVIDE A CHECK ON OVERREACHING GOVERNMENT SURVEILLANCE

The Fourth Amendment requires a warrant, judicial supervision, and protective procedures for government surveillance of communications. See *Berger v. New York*, 388 U.S. 41 (1967). Wiretapping legislation implements these constitutional requirements by setting forth a comprehensive scheme for judicial oversight of communications surveillance. Wiretap laws also impose civil liability on communications service providers to ensure that they act as guardians of customer communications by refusing unlawful surveillance requests. Congress prohibited service providers from entering into secret collaborations with government, in no small part because those collaborations violate the Constitution.

A. Communication Surveillance is so Sensitive that it Receives even Greater Protection than Other Kinds of Searches Under the Fourth Amendment

Customers have a constitutional expectation of privacy in the content of communications, such that surveillance requires judicial approval, supervision and protective procedures. Electronic surveillance requires even greater protections

than other kinds of searches. In *Berger v. New York*, the U.S. Supreme Court required detailed procedures to protect communications privacy under the Fourth Amendment. 388 U.S. 41 (1967). As with other Fourth Amendment searches, the Court required any court order approving electronic surveillance to be issued only upon a finding of probable cause and that applications for court orders state with particularity the offense, the place to be searched, and the things to be seized. *Id.* at 54-56. In addition, the Court required that electronic surveillance investigations be no longer than necessary and that they cease upon finding the sought-after information. *Id.* at 59-60. The Court emphasized that surveillance may only be conducted under "adequate judicial supervision or protective procedures." *Id.* at 60.

Approximately six months later, in *Katz v. United States*, 389 U.S. 347 (1967), the Court held that intercepting a conversation in a phone booth constituted a "search and seizure" under the Fourth Amendment, even though the officers did not physically intrude into an area where the subject had an expectation of privacy. Katz's privacy rights in his intangible telephone conversations triggered the constitutional protections established in *Berger*. Together, *Berger* and *Katz* establish strong constitutional protections for customer communications flowing through facilities owned by AT&T.

B. Following *Berger*, Congress Imposed Civil Liability on Service Providers to Ensure that They Act As Guardians of Consumer Privacy by Refusing to Participate in or Assist Illegal Surveillance

Wiretapping legislation implements constitutional requirements and imposes civil liability on communications service providers to ensure that they act as guardians of customer communications. Following *Berger* and *Katz*, there was a vigorous national debate on whether to allow wiretapping and how to ensure that the power was not abused. Congress decided to permit communications interceptions only for law enforcement purposes in the Wiretap Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212.[1] (Hereinafter, the Wiretap Act – both as originally passed and as amended by ECPA and later statutes – is referred to as "Title III".) Title III subjected surveillance to elaborate safeguards to implement *Berger's* constitutional prerequisites, and strictly limited the use of electronic surveillance by government, service providers and private parties alike.

Like other searches, communications surveillance requires a reviewing judge to find probable cause to believe the target "is committing, has committed, or is about to commit" an offense and that the surveillance will obtain incriminating communications about the offense. 18 U.S.C. 2518(3). But, following *Berger*, Congress added other wire and oral communications interception safeguards as

[1] Congress left national security surveillance unregulated, see Pub. L. No. 90-351, chapter 119, 82 Stat. 214 (1968) (18 U.S.C. 2511(3) (1968)), until revisiting the issue in 1978 with the passage of FISA, see discussion infra at 11-12.

well. Warrants are only available for certain enumerated offenses, not for any crime. *Id.* Interception is a last resort, only after conventional techniques have failed. See 18 U.S.C. 2518(3)(c). Agents must minimize the interception of non-incriminating communications. 18 U.S.C. 2518(5). The investigation must terminate as soon as the sought-after information is acquired, and in any case within thirty days, unless an extension is granted. *Id.* The Act requires notice to targets, which may be delayed until the investigation is complete. See 18 U.S.C. 2518(8)(d). In short, it mandates the extensive involvement of a judicial officer in the entire process. See Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 32 (2004).

Title III also imposes heavy penalties on service providers for intercepting customer communications. Any person who violates Title III is subject to a significant fine and jail time. 18 U.S.C. 2511(1)(d). In addition, Title III gives any person whose communications are illegally intercepted, disclosed, or used standing to bring civil claims for statutory damages or punitive and actual damages, and attorney's fees. 18 U.S.C. 2518(10), 2520. Congress imposes these heavy penalties to deter unlawful surveillance. In 1970, an amendment to Title III exempted service providers from liability for aiding properly authorized law enforcement agents in surveillance. District of Columbia Court Reform and Criminal Procedure Act of 1970, Pub. L. No. 91-358, 211(a), 84 Stat. 473, 654 (1970) (current version

at 18 U.S.C. 2511(2)(a)(ii)). The 1970 amendment accords with the original purpose of Title III, in that it permits surveillance only after judicial approval and only with ongoing judicial supervision.

Congress used the same safeguard, the imposition of heavy civil penalties on service providers who assisted in unlawful interceptions, to ensure intimate judicial supervision of surveillance conducted for national security purposes. In the 1972 case of *United States v. United States District Court for the Eastern District of Michigan ("Keith"),* the government claimed that the President had the authority to conduct national security surveillance without prior judicial approval. *Keith,* 407 U.S. 297 (1972). The U.S. Supreme Court rejected this argument, holding that the Fourth Amendment requires prior judicial review for domestic surveillance — even for national security purposes. *Id.* at 323.

In the *Keith* ruling, the Court suggested that the requirements of national security searches may differ from law enforcement investigations and that Congress could enact a statutory framework to codify different surveillance procedures from those delineated in Title III. However, prior judicial review was not optional. See *Keith,* 407 U.S. 297, 323-324.

The Supreme Court did not reach the question of foreign power surveillance in *Keith*. See *Keith*, 407 U.S. 297, at 322 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign

powers or their agents."). Like the aggrieved parties in *Keith*, neither Plaintiffs nor consumers represented by *amici* are "agent[s] of a foreign power"—they are simply American consumers who rely on AT&T to protect their private, constitutionally-protected communications.

Following *Keith*, Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978. In FISA, Congress implemented the Fourth Amendment protections required by *Keith* for the domestic surveillance, and backed them up with heavy criminal and civil liability for transgressors, including service providers who failed to protect customer communications from warrantless surveillance. FISA created a foreign intelligence surveillance court and guidelines for obtaining surveillance warrants from the court under 50 U.S.C. 1803-1805. As with Title III, Congress made it a crime to violate FISA and gave aggrieved parties standing to sue anyone, including service providers, who intercepted, disclosed or use their communications in violation of the statute. See 50 U.S.C. 1809, 1810.

Congress also amended Title III in 1978 to comport with FISA in two relevant ways. First, it added a section absolutely prohibiting surveillance unless authorized and conducted under the rules and regulations of either Title III or FISA:

> 18 U.S.C. 2511(2)(f) ... procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the **exclusive means** by which electronic surveillance, as defined in section 101 of such Act, and the

> interception of domestic wire and oral communications may be conducted. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (emphasis added).

Second, Congress amended the service provider liability provisions of Title III to include a narrow exception to the requirement of a court order, a "certification". 18 U.S.C. § 2511(2)(a)(ii). This provision made clear that providers would only be shielded from liability for assisting in warrantless surveillance in those rare occasions where FISA and Title III allow limited surveillance in advance of delayed judicial review. These situations are limited to (1) emergency FISA surveillance where a court order is obtained within 72 hours (50 U.S.C. 1805(f)); (2) emergency Title III surveillance where an application for court order is made within 48 hours (18 U.S.C. 2518(7)); (3) warrantless FISA surveillance for up to one year, where solely directed and foreign powers with no substantial likelihood of acquiring U.S. persons' communications (50 U.S.C. 1802); and (4) warrantless FISA surveillance fifteen days following declaration of war (50 U.S.C. 1811). The "certification" amendment did not alter in any way Congress' clear edict that surveillance of American citizens be subject to judicial review and that service providers that failed to ensure review would ultimately answer to the courts. See Plaintiffs Opposition to AT&T Corp's Motion to Dismiss, docket 176, pp. 15-17, available at <http://www.eff.org/legal/cases/att/oppositiondismisscorp.pdf>.

In 1986, Congress extended some of the wiretapping protections to electronic communications, and thus gave persons aggrieved by unlawful interception of those electronic communications the right to sue the entities involved. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (current version at 18 U.S.C. 2510 *et seq.*). ECPA's Stored Communications Act (SCA) created service provider liability for disclosing the contents of "a communication while in electronic storage" or the contents of "any communication which is carried or maintained on [a remote computing] service" without a warrant. *Id.* at 1861 (codified at 18 U.S.C. 2702, 2703 (communications older than 180 days can be obtained with a warrant or with notice and a subpoena or court order). The SCA as amended also extends liability to service providers for divulging "record[s] or other information pertaining to a subscriber to or a customer of such service...to any governmental entity." 18 USC 2702(a)(3).

Title III (including the SCA) and FISA place service providers squarely in the role of guardians of customer communications. Congress has never deviated from its initial scheme to protect constitutional privacy rights in communications by requiring a pre-surveillance warrant and elaborate judicial supervision, backed up by criminal and civil penalties for any person, including service providers, who breaks the law. These penalties demonstrate Congress' commitment to eradicating

unlawful surveillance by the government and private parties.

C. Congress Set Up This Scheme with the Intention of Making Service Providers Guardians of Consumer Communications Privacy and Giving Them Powerful Incentives to Resist Unlawful or Excessive Government Surveillance

Following *Berger,* Congress authorized surveillance only under narrow circumstances and only with pre-surveillance judicial approval and significant continuing judicial oversight. Congress wanted to assure "the responsible part that the judiciary must play in supervising the interception of wire or oral communications in order that the privacy of innocent persons may be protected." S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2177. Congress emphasized the importance of Title III's statutory procedures by stating that "[j]udicial review of the decision to intercept wire or oral communications will not only tend to insure that the decision is proper, but it will also tend to assure the community that the decision is fair." S. Rep. No. 90-1097 (1968), *as reprinted in* U.S.S.C.A.N. 2112, 2185. Such precautions are fundamental in a democracy.

Congress has approved additional communications surveillance bills proposed by the Executive Branch that maintain service providers as strong guardians of consumer privacy. When law enforcement lobbied Congress for rules requiring telecommunications providers to alter their facilities to enable the government to expeditiously intercept digital wire and electronic communications

as part of the Communications Assistance to Law Enforcement Act (CALEA), Congress agreed because it assumed that service providers would continue to safeguard Americans' private thoughts and messages from the government.

For example, before the Judiciary Subcommittee on Technology and the Law, Bill O'Malley (President of the National District Attorneys Association) testified that "...the very industry whose help we seek today serves as a protective balance. I can assure you that local law enforcement does not have the capability to directly intercept telephonic communications and that the telecommunication industry will not provide the requested technical assistance in the absence of a court order." Joint Hearing Before the S. Judiciary Subcomm. on Technology and the Law and the H. Subcomm. on Civil and Constitutional Rights, 103rd Cong., 2d Sess. (1994) (testimony of William C. O'Malley, Pres. of the Nat'l Dist. Att'ys Assn).

Similarly, Louis J. Freeh (Director of the Federal Bureau of Investigation) also assured consumers that the new law included "the basic requirement that carriers fulfill their electronic surveillance assistance requirements in a manner that protects the privacy and security of communications and information of all subscribers whose communications are not authorized to be intercepted"[2], that

[2] Implicitly codified under 47 U.S.C. 1002(a)(1) ("to the exclusion of any other communications").

"there are systems security provisions which enhance privacy and security by requiring that all electronic surveillance efforts initiated in switching premises be activated only with the affirmative intervention of a carrier employee"[3] and that "enhanced privacy protection[4] is included with regard to governmental access to any interactive transactions for which a carrier may keep a record." See Joint Hearing Before the S. Judiciary Subcomm. on Technology and the Law and the H. Subcomm. on Civil and Constitutional Rights, 103rd Cong., 2d Sess. (1994) (testimony of Louis J. Freeh, Dir. of the Fed. Bureau of Investigation)

Congress relied on the fact that service providers have both the technological capacity and the legal incentives to safeguard communications and refuse unlawful surveillance when it approved CALEA. "[The proposed CALEA bill] ... [r]equires affirmative intervention of common carriers' personnel for switch-based interceptions—this means law enforcement will not be able to activate interceptions remotely or independently within the switching premises of a telecommunications carrier." H.R. Rep. No. 103-827, pt. 1, at 4 (1994). Similarly, Representative Edward J. Markey (D-MA) commented that "Section 105 [of CALEA] represents a significant expansion of privacy protection for citizens

[3] Implicitly codified under 47 U.S.C. 1002(c) (requiring that monitoring won't take place on the premises of service providers, except in cases of emergency or exigent circumstances).

[4] Implicitly codified under 47 U.S.C. 1002(a)(4)(A).

everywhere. It ensures that wiretapping technology does not become so easy as to obviate the need for telephone company participation, which serves as a check against an end-run of the judicial system." 140 Cong. Rec. H10773-02, H10781 (daily ed. Oct. 4, 1994) (statement of Rep. Markey) (codified at 47 U.S.C. 1004).

The Constitution and wiretap statutes call for significant judicial involvement in surveillance. Service providers can grant or deny government access to communications because they own the facilities through which our protected messages flow. Because of this unique power, Congress made service providers the guardians of consumer privacy, by creating criminal and civil penalties for unlawful interception, disclosure and use. The whole purpose of this scheme is to ensure that service providers do not secretly give government agents warrantless access to consumer communications and communications records. Service providers must check for a court order or a valid certification that none is needed, to ensure that surveillance is conducted constitutionally and only under appropriate judicial supervision. The service provider is the only practical check on overreaching law enforcement surveillance, and it performs this role because if it does not, it will be liable.

II. LIABILITY IS CRITICAL TO DETER SERVICE PROVIDER COLLUSION IN ILLEGAL SURVEILLANCE

Consumer lawsuits such as this one vindicate important Constitution-based privacy rights, not mere private interests. Customers trust companies to protect their communications privacy. When telecommunications companies like AT&T secretly conspire with the government to breach that trust, customers need civil liability to penalize lawlessness and to limit government abuses.

A. Civil Liability is the Only Effective Deterrent for Secret Illegal Surveillance

Public opinion polls consistently find Americans strongly support privacy laws to protect their personal information from commercial entities and government. See, e.g. EPIC, Public Opinion on Privacy, *available at* http://www.epic.org/privacy/survey/. For example, the Graphic, Visualization, & Usability Center's 10th WWW User Survey reported that 93% of study participants agreed with the statement, "I ought to be able to communicate over the Internet without people being able to read the content." GVU's WWW User Surveys, Privacy of Communications, *available at* http://www.gvu.gatech.edu/user_surveys/survey-1998-10/. Similarly, in a USA Today / Gallup Poll, 57% of respondents would feel their privacy had been violated if they found that their phone company had turned their records, not even

the content of their messages, over to the government as part of a program to create a database of phone numbers. USA Today, Government Phone Records Reaction, May 2006, *available at* http://www.usatoday.com/news/polls/tables/live/2006-05-14-nsa-poll.htm. Sixty two percent favored immediate Congressional hearings investigating that program. *Id.*

Providers have strong natural motivations to acquiesce to government requests for access to customer communications, whether legal or not. Cooperation is smart business, since government taxes and regulates service providers. No wonder, as *Amici* Chamber of Commerce admits "[for the most part], industry willingly cooperates in national security programs and activities, including those that are classified." Chamber of Commerce *Amicus* Brief, p. 9-10.

When customers know a company's business practices and can choose among competitors, they can use their purchasing power to force companies to adopt more privacy-friendly practices. For example, as a result of consumer complaints, America Online and Earthlink no longer maintain clickstream data. See Christopher Slobogin, Subpoenas and Privacy, 54 DePaul L. Rev 805, 836 n. 161 (2005), *citing* Conversation with Peter P. Swire, Professor of Law, Ohio State University Moritz College of Law, Sept. 20, 2004, at Ohio State College of Law. When Amazon.com announced a new feature that would reveal what customers in particular cities, schools, or corporations were reading, news reports focusing on

privacy concerns forced the company to announce a new opt-out plan. Jessica Litman, *Information Privacy/Information Property*, 52 Stan. L. Rev. 1283, 1305–07 (2000) (detailing examples of businesses bowing to pressure to stop using personal data for marketing purposes including consumer protests forcing AOL to abandon plans to sell subscriber phone numbers, and RealNetworks abandoning software that collected information about the user's downloading, recording, and listening behavior.)

This market dynamic is too weak to stop illegal, secret communications surveillance. First, providers and government have colluded to keep their surveillance practices secret. Customers cannot effectively exercise choice when the facts are hidden from them.

Second, citizens have little to no control over the path their communications take on the network. AT&T is the largest telecommunications and broadband DSL Internet service provider in the United States. See Amended Complaint, Feb. 22, 2006, ¶¶ 27-28. By the end of 2004, AT&T provided services for 300 million voice calls per business day—generating approximately 200 times the amount of data contained in all the books in the Library of Congress. *Id.*, at ¶ 24. Even if a particular individual chooses to boycott AT&T, the people with whom she is communicating probably still use the service, and that means her communications with those friends are captured despite her desire to opt out. Furthermore, many

communications providers lease facilities from AT&T, and billions of email messages are routed through AT&T's backbone internet network, regardless of customer choice. Consumers simply cannot choose to stop AT&T from carrying their communications, despite considerable public outrage.[5]

Finally, unlike collecting click-stream data or disclosing customer preferences, warrantless communications interception violates the law. Illegal activity demands a stronger rebuke than the market can bring to bear. For these reasons, consumers need civil liability to encourage service providers to guard their privacy.

B. Civil Liability Does No Harm to Legitimate Government-Industry Cooperation

When the government has critical national security objectives, it can conduct legal surveillance under Title III or FISA. Short of that, defendant AT&T's duty is to deny government's requests to violate consumer privacy. The Constitution, Title III and FISA work together to require service providers to protect the content of communications unless and until a judge says otherwise. Failure to do so is illegal and dangerous.

[5] See, e.g., Zogby International, New Zogby Poll Shows Majority of Americans Support Impeaching Bush for Wiretapping, *available at* http://www.zogby.com/search/ReadClips.dbm?ID=12525.

Defendant's *amici* misunderstand that the very purpose of the Fourth Amendment and Title III is to deter illegal wiretapping. For example, *amici* U.S. Telecomm Ass'n frets that the trial court's ruling will "discourag[e] private actors from assisting the Government in obtaining intelligence." USTA *Amicus* Brief at p. 22. That is the exact purpose of Title III and its amendments. This legislation specifically functions to deter service providers from blindly cooperating with the government. Blind cooperation to law enforcement requests does not make service providers "good corporate citizens". See *id.* at p. 3. Good corporate citizens work with the government within the boundaries of law and protect the rights and expectations of their customers.

Congress explicitly disavowed the "good-corporate-citizen-just-taking-orders" excuse when it established the statutory good faith defense at 18 U.S.C. 2520(d) as the exclusive means by which a telecommunications provider may raise its cooperation with the government as a defense to liability. Only a good faith reliance on (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7); or (3) a good faith determination that section 2511(3) or 2511(2)(i) permitted the conduct complained of is a defense against any civil or criminal action brought under any legal authority.

In *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978), the Ninth Circuit rejected AT&T's "secret relationship" defense in favor of the carefully crafted cooperation defense established in section 2520. In *Jacobson*, phone company Nevada Bell resisted civil liability on the grounds that it should not be punished for helping the government. The Court held that a good faith defense for provider cooperation with law enforcement could only lie under section 2520, and no other theory.

> We appreciate [Nevada] Bell's concern that it may be held liable for cooperating with the police at the request of the Nevada state court. But the proper response to that concern is not to emasculate the statute. Congress appreciated this potential dilemma and established a defense for good faith reliance on a court order. It is upon such a defense that Bell must rely. *Id.* at 522.

Jacobson rejects AT&T's and its *amicis'* argument that service providers can defend themselves on the grounds that the government told them to do it. Congress considered the need for provider/government cooperation and carefully crafted both the scope of liability for and available defenses to telecommunications providers. Section 2520 forecloses any argument that courts can superimpose some form of "absolute common-law immunity" on top of Congress's statutory scheme.

The choice this Court makes is not between "critical national security objectives and a private lawsuit", but between unjustified, unauthorized and unsupervised mass surveillance and the constitutional and statutory privacy rights of all Americans. National security requires cooperation, but that cooperation must be legal and respectful of the Constitution. *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) [Even "… a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens."] All the examples defendant's *amici* give (e.g., development of weapons, aircraft, aircraft identification technology and anti-missile systems needed by the U.S. Military, manufacture of underwater coupling device for fiber optics, development of stealth technology aircraft, the Manhattan Project) are legal activities of the government, do not require judicial approval or review and don't implicate the constitutional rights of American citizens. See Chamber of Commerce *Amicus* Brief, pp. 6-9.

III. CONCLUSION

The Constitution requires government to submit to judicial supervision of communications surveillance. Service providers like AT&T are in a unique position because they own the pipes through which consumer communications flow, so only service providers can ensure that surveillance is conducted properly. In Title III and FISA, Congress imposed civil liability on service providers to

incentivize them to guard against government overreaching. Congress trusts government with surveillance powers exactly because it assumes that providers will safeguard consumer privacy, and consumers feel the same way. There is no place in this scheme for "secret relationships" that betray consumers, the Constitution and Congress. AT&T must be held liable or citizens will have no protection from the government illegally intruding on their most intimate and personal messages and thoughts.

For these reasons, this Court should affirm the District Court's order denying AT&T's and the government's motions to dismiss.

Dated: May 2, 2007 Respectfully Submitted,

_____

Jennifer Stisa Granick
Lauren Gelman
Shannon Kenealy, Law Student
CYBERLAW CLINIC
CENTER FOR INTERNET AND SOCIETY
STANFORD LAW SCHOOL
Crown Quadrangle
559 Nathan Abbott Way
Stanford, California 94305-8610
Telephone: (650) 724-0014
Facsimile: (650) 723-4426

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 29(d) and 9th Cir. R. 32-1, the attached amicus brief is proportionally spaced, has a typeface of 14 points or more and contains 5,105 words or less. This certificate was prepared in reliance on the word court of the word-processing system (Microsoft Word) used to prepare this brief.

_____

Lauren Gelman

CERTIFICATE OF SERVICE

I, Amanda Smith, the undersigned, do hereby state that on May 2, 2007, I caused to be served the within:

AMICI CURIAE BRIEF OF CONSUMER RIGHTS GROUPS: CENTER FOR DIGITAL DEMOCRACY, CONSUMER FEDERATION OF AMERICA, CONSUMERS UNION, PRIVACYACTIVISM AND U.S. PUBLIC INTEREST RESEARCH GROUP IN SUPPORT OF APPELLEES

on counsel listed below by depositing two true copies thereof, enclosed in a sealed envelope via Federal Express for overnight delivery at Palo Alto, California, to each person listed below addressed as follows:

Peter D. Keisler <peter.d.keisler@usdoj.gov>
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue N.W.
Room 6102
Washington, D.C. 20001
(202) 514-4782 (tel.)
(202) 616-8470 (fax)

Douglas N. Letter <Douglas.Letter@usdoj.gov>
U.S. Department of Justice
Civil Division, Appellate Staff
950 Pennsylvania Avenue N.W.
Room 7513
Washington, D.C. 20530-0001
(202) 514-3602 (tel.)
(202) 514-8151(fax)

Paul D. Clement
Office of the Solicitor General
950 Pennsylvania Avenue NW
Suite 5143
Washington, D.C. 20530-2201

(202) 514-2201 (tel.)
(202) 514-3648 (fax)

Bruce A. Ericson <bruce.ericson@pillsburylaw.com>
Pillsbury Winthrop Shaw Pittman LLP
50 Fremont Street
San Francisco, CA 94105
(415) 983-1000 (tel.)
(415) 983-1200 (fax)

Michael K. Kellogg <mkellogg@khhte.com>
Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C.
1615 M. Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900 (tel.)
(202) 326-7999 (fax)

Cindy Cohn
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 (tel.)
(415) 436-9993 (fax)

Robert D. Fram
Heller Ehrman LLP
333 Bush Street
San Francisco, CA 94104
(415) 772-6000 (tel.)
(415) 772-6268 (fax)

Jonathan B. Banks
United States Telecom Association
607 14th Street, N.W., Suite 400
Washington, D.C. 20005
(202) 326-7300 (tel)
(202) 326-7333 (fax)

Andrew G. McBride
Wiley Rein, LLP

1776 K. Street, N.W.
Washington, D.C. 20006
(202) 719-7000 (tel.)
(202) 719-7049 (fax)

Robin S. Conrad
National Chamber Litigation Center, Inc.
1615 H. Street, N.W.
Washington, D.C., 20062
(202) 463-5337 (tel.)

Herbert L. Fenster
McKenna Long & Aldridge, LLP
1900 K. Street, N.W.
Washington, D.C., 20006
(202) 496-7500 (tel.)

Executed on May 2, 2007 at Palo Alto, California. I declare under penalty of perjury that the foregoing is true and correct.

_____

Amanda Smith