at&t

Wayne Watts
Senior Executive Vice President and General Counsel

AT&T Inc.
175 East Houston
Suite 1306
San Antonio, TX 78205

T: 210.351.3300
F: 210.351.2298
wayne.watts@att.com

October 12, 2007

The Honorable John D. Dingell
The Honorable Edward J. Markey
The Honorable Bart Stupak
Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Congressmen Dingell, Markey and Stupak:

I am responding to your letter to Randall Stephenson, Chairman and CEO of AT&T Inc., dated October 2, 2007, regarding AT&T's policies and practices with respect to governmental requests for law enforcement or intelligence assistance pursuant to the Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and other sources of law. We are pleased to have the opportunity to share with you our perspective on these important issues.

We understand and respect your interest in the subjects about which you inquire. Unfortunately, under current circumstances, we are unable to respond with specificity to your inquiries. That is because, on many issues that appear to be of central concern to you, responsive information, if any, is within the control of the executive branch. For example, if such information were to exist, AT&T could not lawfully furnish classified information in this response. Indeed, we are not in a position even to confirm or deny the existence of any underlying facts or information that would be responsive to your requests that could be considered classified. Moreover, the United States, through a sworn declaration from the Director of National Intelligence (DNI), has formally invoked the state secrets privilege to prevent AT&T from either confirming or denying certain facts about alleged intelligence operations and activities that are central to your inquiries. As such, no conclusions can or should be drawn from this letter about the existence or non-existence of information that could be responsive to your requests.

The state secrets privilege is an ancient privilege of constitutional dimension – its antecedents in American law date back to the treason trial of Aaron Burr – that allows the executive to prevent disclosure of military, intelligence, or diplomatic secrets whose disclosure could harm the country's security. *See, e.g., El-Masri v. United States*, 479 F.3d 296, 303 (4th Cir. 2007). Under the law, only the executive can waive this privilege or reach accommodations with the Congress to share information that is subject to it. *See United States v. Reynolds,* 345 U.S. 1, 7-8 (1952) ("The privilege . . . can neither be claimed nor waived by a private party."). On the subjects that are the focus of your letter, the state secrets privilege was invoked based on an express conclusion by the

DNI that certain categories of defense-related information, if disclosed, would severely harm the country's safety and security. Federal felony sanctions attach to any unauthorized disclosure of such information. 18 U.S.C. § 793(d).

As a private party cooperating with a congressional request, AT&T is prohibited by law in other respects, too, from disclosing certain sensitive law enforcement or intelligence information without leave of the executive branch. It would, for example, be a federal felony for AT&T to set forth in this letter any classified information "concerning the communications intelligence activities of the United States." 18 U.S.C. § 798(a)(3). We are likewise statutorily prohibited from disclosing "the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to" certain categories of authorized government intelligence-gathering activity. 18 U.S.C. § 2511(2)(a)(ii). Under 18 U.S.C. § 2709(c)(1), we cannot disclose the existence of certain National Security Letters (NSLs); the statute specifically directs that information of that type be furnished to the Congress by the FBI itself, *see* 18 U.S.C. § 2709(e). Likewise, under the FISA statute, we are forbidden from disclosing information pertaining to the FBI's use of FISA business records; such information is also statutorily controlled by the FBI. 50 U.S.C. § 1861(b)(1). And there are unique protections in the law for any and all information pertaining to "the organization or any function of the National Security Agency, or any information with respect to the activities thereof." 50 U.S.C. § 402 note; *see also The Founding Church of Scientology of Washington, D.C., Inc. v. National Sec'y Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Hayden v. National Sec'y Agency*, 608 F.2d 1381, 1389 (D.C. Cir. 1979); *Linder v. National Sec'y Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996). Given the strictness of many of these prohibitions, the seriousness of the sanctions for violating them, and the uncertainty with respect to the manner in which they apply to the questions in your letter, our response is necessarily limited.

Given the focus of your questions, our company essentially finds itself caught in the middle of an oversight dispute between the Congress and the executive relating to government surveillance activities. We value our good working relationship with the Congress and with your committees. Nevertheless, applicable legal rules make clear that much of the information you seek is under the control of the executive and that disputes of this kind need to be resolved through accommodation between the two political branches of government.

Within the boundaries imposed by the legal constraints we face, I can share with you some observations concerning law enforcement and intelligence assistance which may be lawfully provided by companies such as ours. In the midst of the current controversy over the NSA's alleged surveillance activities, there is a tremendous amount of misinformation and misunderstanding surrounding this general topic. Nonetheless, the broad outlines of national policy are clear, consistent, and long-standing: telecommunications carriers are authorized to assist government agencies in a wide variety of circumstances, only some of which require judicial process; public policy encourages such cooperation, which has traditionally been regarded as being in the public interest; and, consistent with that policy, when a carrier cooperates in good faith

with a duly authorized request for assistance, the carrier is immune from any form of liability to third-parties.

Contrary to some of the current public discourse, the circumstances under which telecommunications carriers are authorized by law to share information with the government are not limited to a small number of straightforward categories. Nor are they limited to circumstances in which a warrant or other court order has issued. In many situations, communications providers are authorized to share information with law enforcement or intelligence agencies without the involvement of any court, including the Foreign Intelligence Surveillance Court.

At the federal level, carriers may furnish government agencies access to telecommunications content or records pursuant to such varying forms of process as judicial warrants, subpoenas, Title III orders, FISA orders, Attorney General certifications, administrative subpoenas and NSLs, and other statutory authorizations. The principal statutory authorities for lawfully sharing information with agencies of the federal government include, but are not limited to, the following:

- Pursuant to 18 U.S.C. §§ 2516 and 2518, a communications provider is authorized to intercept communications when a Title III order is issued by a court in connection with certain criminal investigations;

- Pursuant to 18 U.S.C. § 2511(2)(a)(ii), a communications provider is authorized to provide information, facilities, or technical assistance to authorized law enforcement or intelligence officials upon receipt of a court order or an appropriate certification from the Attorney General that no warrant or court order is required;

- Pursuant to 18 U.S.C. §§ 2511(2)(a)(ii) and 2518(7), a communications provider is authorized to provide information, facilities, or technical assistance to authorized law enforcement or intelligence officials without a court order in emergency circumstances involving national security conspiracies, organized crime, or immediate danger to life and limb;

- Pursuant to 18 U.S.C. § 2511(3)(b)(iv), a communications provider is authorized to provide without a court order the contents of communications that were inadvertently obtained and that appear to pertain to the commission of a crime;

- Pursuant to 50 U.S.C. §§ 1804 and 1805, a communications provider is authorized to allow foreign intelligence surveillance of certain categories of communications with a U.S. nexus with an order from the Foreign Intelligence Surveillance Court;

- Pursuant to 50 U.S.C. § 1802(a), a communications provider is authorized to furnish information, facilities, and assistance to allow foreign intelligence surveillance of certain categories of communications with a U.S. nexus without a court order upon certification by the Attorney General that the surveillance is

directed at communications exclusively among foreign powers and is unlikely to capture any communications of U.S. persons or involves technical collection against property openly controlled by a foreign power;

- Pursuant to 50 U.S.C. § 1805(f), a communications provider is authorized to allow foreign intelligence surveillance of certain categories of communications with a U.S. nexus without a court order when the Attorney General reasonably determines that an emergency situation exists and that the standards for a FISA court order could be met;

- Pursuant to 50 U.S.C. § 1811, a communications provider is authorized to allow foreign intelligence surveillance of certain categories of communications with a U.S. nexus without a court order upon receipt of an Attorney General authorization following a declaration of war;

- Pursuant to 50 U.S.C. § 1861, a communications provider is authorized to provide business records, including customer information, for counterterrorism purposes pursuant to a FISA order;

- Pursuant to the terms of the recently-enacted Protect America Act of 2007, Pub. L. No. 110-55, which is of temporary duration, a communications provider is authorized to furnish information, facilities, and assistance to enable foreign intelligence surveillance directed at targets reasonably believed to be outside the United States without a court order upon certification by the DNI or Attorney General;

- Pursuant to 18 U.S.C. §§ 2702(b)(5) and 2702(c)(3), a communications provider is authorized to disclose stored customer communications or records to the government when necessary to protect the rights or property of the provider;

- Pursuant to 18 U.S.C. §§ 2702(b)(6) and 2702(c)(5), a communications provider is authorized to disclose stored customer communications or records to the National Center for Missing and Exploited Children in connection with certain statutory reports;

- Pursuant to 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4), a communications provider is authorized to disclose stored customer communications or records to the government based on a good faith belief that an emergency exists involving danger to life or limb;

- Pursuant to 18 U.S.C. §§ 2703(a) and (c), a communications provider is authorized to disclose stored communications reasonably believed to be relevant to a criminal investigation upon receipt of a judicial warrant or a court order pursuant to 18 U.S.C. § 2703(d);

- Pursuant to 18 U.S.C. §§ 2703(c)(1)(D), a communications provider is authorized to disclose records pertaining to a customer in conjunction with investigations of telemarketing fraud or pursuant to administrative subpoena;

- Pursuant to 18 U.S.C. § 2709, a communications provider is authorized to disclose subscriber information and billing records upon receipt of an NSL from the FBI in connection with counterintelligence and counterterrorism investigations;

- Pursuant to 50 U.S.C. § 1842 and 18 U.S.C. § 3127, a communications provider is authorized to permit government agencies to install and use pen register and trap-and-trace devices upon receipt of appropriate court orders;

- Pursuant to 50 U.S.C. § 1843, a communications provider is authorized to permit government agencies to install and use pen register and trap-and-trace devices in emergency circumstances for counterterrorism purposes against non-U.S. person targets without a court order upon request of the Attorney General;

- Pursuant to 50 U.S.C. § 1844, a communications provider is authorized to permit government agencies to install and use pen register and trap-and-trace devices without a court order upon receipt of an Attorney General authorization following a declaration of war.[1]

In addition to these statutory authorities, the President possesses independent authority to request intelligence assistance pursuant to his recognized constitutional responsibility to conduct the nation's foreign policy and to protect it from foreign threats. *See, e.g., In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (describing the President's inherent constitutional authority to gather foreign intelligence information). As we understand it, Congress accepts and has never sought to regulate this authority (including in the FISA statute) insofar as it relates to the gathering of foreign, military, or diplomatic intelligence against foreign targets outside the United States. *See, e.g.*, 18 U.S.C. § 2511(f) (recognizing that federal statutes do not purport to affect the President's acquisition of foreign intelligence information from international or foreign communications by means other than electronic surveillance as defined in FISA). Thus, in addition to the statutory authorities cited above, the President or other executive branch officials might request various forms of intelligence assistance from the private sector pursuant to Executive Order 12333 and/or the President's Article II powers on which that Order rests.

Even this does not begin to exhaust the wide variety of circumstances under which a carrier might be obliged to furnish assistance. For example, in a kidnapping or a hostage situation, it may be appropriate for law enforcement to ask for exigent

---

[1] You have asked about remuneration received by companies furnishing assistance to the federal government. As a general matter, such companies are statutorily entitled to receive nominal remuneration on the basis of either reasonable cost recovery or fair compensation at prevailing rates depending upon the assistance and facilities they provide. *See, e.g.*, 18 U.S.C. §§ 2518(4), 2706; 50 U.S.C. § 1802(a)(4); Protect America Act, Pub. L. No. 110-55 § 105B(f). AT&T's Court Order Bureau in Kansas City is reimbursed on such a basis.

assistance in monitoring a communication. The law allows law enforcement to make, and for telecommunications carriers to respond to, these kinds of requests, with provision of an appropriate court order only after-the-fact.

AT&T is committed to providing assistance to the government strictly in accordance with law. AT&T has an organization in place to ensure that we provide timely, responsible, and lawful assistance to the government to help protect members of the public. To comply with authorizations for lawful electronic surveillance, federal law requires AT&T to install and maintain the capability and capacity to assist the government in electronic interception of communications when such interceptions are required to be accomplished with AT&T's own equipment. *See* Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002; 18 U.S.C. §§ 2518(4), 2522 ("CALEA"). In other circumstances, government agencies may use their own equipment to accomplish authorized surveillance. With respect to requests for call detail records ("CDRs"), we currently employ software and hardware and other procedures that prevent the disclosure of CDRs only where AT&T has been served with a lawful request. AT&T staff insures that the disclosed data comports with the associated legal demands. AT&T's staff also receives appropriate training on these procedures.

When a carrier such as AT&T responds to duly authorized requests for assistance from law enforcement or intelligence agencies in a good faith belief that the requested assistance is lawful, it has been the considered and consistent legal and policy judgment of Congress and the courts that no liability should attach to the carrier. That is true even if the government or government officials are subsequently determined to have acted unlawfully. For example, in *Smith v. Nixon*, 606 F.2d 1183 (D.C. Cir. 1979), Judge Skelly Wright of the United States Court of Appeals for the District of Columbia upheld the dismissal of the Chesapeake & Potomac Telephone Company from a case challenging the government's wiretapping of a home telephone. The court strongly suggested that the government's request for the wiretap was illegal, yet the Court of Appeals ruled that "C&P's limited technical role in the surveillance as well as its reasonable expectation of legality cannot give rise to liability for any statutory or constitutional violation," because "[t]he telephone company did not initiate the surveillance, and it was assured by the highest Executive officials in this nation that the action was legal." *Id.* at 1191.

This same principle – that a telecommunications carrier who cooperates in good faith with authorized law enforcement or intelligence activities considered lawful by the executive – underlies numerous defenses and immunities reflected in existing statutory and case law.[2] For example, 18 U.S.C. § 2511(2)(a)(ii) provides that "*[n]otwithstanding*

---

[2] *See, e.g.*, 18 U.S.C. §§ 2511(2)(a)(ii), 2520(d), 2703(e), 2707(e); 50 U.S.C. §§ 1805(i), 1842(f), 1861(e); Protect America Act, Pub. L. No. 100-55 § 105B(l); *Smith v. Nixon*, 606 F.2d 1183, 1191 (D.C. Cir. 1979); *Halperin v. Kissinger*, 424 F. Supp. 838, 846 (D.D.C. 1976), *rev'd on other grounds*, 606 F.2d 1192 (D.C. Cir. 1979); *see generally Raley v. Ohio*, 360 U.S. 423 (1959); *Cox v. Louisiana*, 379 U.S. 559 (1965); *United States v. Pennsylvania Industrial Chemical Corporation* ("*PICCO*"), 411 U.S. 655 (1973); *United States v. Barker*, 546 F.2d 940, 946 (D.C. Cir. 1976); *Kratz v. Kratz*, 477 F. Supp. 463, 482-83 (E.D. Pa. 1979).

any other law," carriers are authorized to provide "assistance" and "information" to the government whenever the communications service provider receives a "certification" from the Attorney General or his designee "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." When the Attorney General furnishes an appropriate certification, Congress has decreed that "*no cause of action shall lie in any court.*" It does not matter whether the Attorney General's judgment reflected in the certification is ultimately determined to have been right or wrong: as long as the carrier acted pursuant to such a certification, national policy forbids a lawsuit. Congress felt so strongly on this point that it included a supplementary good faith defense, such that the carrier is insulated from liability even if the *carrier itself* is wrong. If a carrier makes "a good faith determination" that it had appropriate statutory permission for its conduct, then it has "a complete defense against any civil or criminal action brought under . . . any . . . law." *Id.* § 2520(d).

Courts have clearly and consistently described the public policies at play when a private citizen reasonably relies on assurances of legality from responsible government officials. In *United States v. Barker*, 546 F.2d 940 (D.C. Cir. 1976), the D.C. Circuit explained:

> [T]he public policy of encouraging citizens to respond ungrudgingly to the request of officials for help in the performance of their duties remains quite strong. Moreover, the gap (both real and perceived) between a private citizen and a government official with regard to their ability and authority to judge the lawfulness of a particular governmental activity is great. It would appear to serve both justice and public policy in a situation where an individual acted at the behest of a government official to allow the individual a defense based upon his reliance on the official's authority—if he can show that his reliance was objectively reasonable under the particular circumstances of the case.

Id. at 948-49 (Wilkey, J.). Judge Merhige, concurring, believed that "the defense advances the policy of fostering obedience to the decisions of certain individuals and groups of individuals that society has put in positions of prominence in the governing structure—*i.e.* courts, executive officials and legislative bodies." *Id.* at 956 (Merhige, J.). In the end, he concluded, it would be unreasonable to "require[] the individual citizen to be more cognizant of and have a better understanding of the law than a public official who is responsible for and specifically employed to make interpretations of the law in the relevant legal field." *Id.* at 957. Taken together, these statutory and common law defenses and immunities reflect a remarkably consistent and emphatic policy judgment that it is unfair to hold carriers responsible for decisions and judgments made by government officials, and inimical to the public interest to discourage companies from providing prompt cooperation to law enforcement and intelligence agencies that require assistance.

The problem, which we have discovered in the recent maelstrom of litigation surrounding the alleged counterterrorism surveillance conducted by the NSA in the

wake of the attacks of September 11th, is that these and other immunities and defenses are sometimes ineffective to bring a swift end to litigation involving state secrets. When the subject matter of the litigation involves allegations of highly classified intelligence activities, private parties are disabled from making the factual showings necessary to demonstrate that the cases lack legal merit. If courts do not swiftly dismiss such cases based on the state secrets privilege, then carriers who are alleged to have cooperated with intelligence activities are faced with years of litigation, at great financial and reputational cost, and are forced to remain mute in the face of extreme allegations, no matter how false. This is so even when the carriers are alleged, as is the situation in the current NSA litigation, to have cooperated with fully authorized intelligence activities that our nation's highest officials have determined to be, and continue to maintain are, legal. Such a situation is exceptionally unfair to the carrier defendants, regardless of whether they actually participated in any intelligence program of the sort alleged.

This legal paradox has implications not just for the carrier defendants, but for the nation's security in general. It suggests to private companies that even good faith cooperation in apparently authorized and lawful intelligence activity can expose them to serious legal and business risks. This creates incentives to resist cooperation with the government that might be vital to saving American lives in the future – incentives that fly in the face of the consistent national policy reflected in existing statutes and case law.

You have specifically asked whether we believe it is proper for the onus to be on a company to determine whether the government is acting within the scope of its authority when it requests customer information. As a general matter, we accept that we have a responsibility to do what we reasonably can to verify that proper process is being employed – for example, that an NSL or subpoena is properly executed and furnished. But as the law cited above reflects, when the government asks for assistance from a telecommunications carrier, primary responsibility for ensuring its legality falls on the government: although carriers should not furnish assistance they know to be unlawful, their responsibilities are primarily procedural in nature.

There are important practical reasons for this, which derive from significant limits on what a carrier can reasonably be expected to do in these situations. Given the high volume of requests a company our size processes each year and the limits of any communications provider's knowledge, it is not feasible for a provider to undertake independent investigations of the facts and circumstances underlying most requests for assistance from the government. A carrier can check to make sure that there is a facially valid subpoena or Title III order, but it cannot determine whether there are defects in the processes used to obtain those documents, or substantive defects in the underlying investigations. A carrier can insist on seeing a facially valid warrant, but it cannot usurp the role of the courts and make its own probable cause determination. And in the foreign intelligence context, companies in the private sector almost certainly will not have access to the underlying operational information that would be necessary to decide complex constitutional questions about the scope of presidential power. Such questions are in any event far outside such companies' institutional expertise.

In short, we take legal compliance very seriously in all aspects of our business, but the law does not assign us the primary responsibility for policing government agencies. Institutions of government, not private companies, play that role. Public officials, not private businessmen, must ultimately be responsible for whether the legal judgments underlying authorized surveillance activities turn out to be right or wrong - legally or politically. Telecommunications carriers have a part to play in guarding against official abuses, but it is necessarily a modest one.

In closing, let me thank you for the opportunity to respond to your inquiries. I hope that we can work together in the coming weeks both to satisfy your legitimate need for information and to provide statutory protection for carriers such as AT&T that have been unfairly targeted in litigation challenging alleged intelligence activities for which only the government can and should be responsible.

Respectfully submitted,

Wayne Watts
Sr. Executive Vice President
and General Counsel

CC: Honorable Joe Barton
Honorable Fred Upton
Honorable Ed Whitfield