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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

Importantly, this Court may properly conclude that plaintiffs' communications have been and are being intercepted even absent knowledge of the exact operational details of [redacted] that are acquiring plaintiffs' communications, or the exact arrangement between the government and AT&T regarding control of those facilities, because "[Title III's] application should not turn on the type of equipment that is used, but whether the privacy of [communications] has been invaded in a manner offensive to the words and intent of the Act." *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979). Nor does it matter whether any human beings personally read or listen to the acquired communications. *See George v. Carusone*, 849 F. Supp. at 163 (finding an interception even though defendants never listened to the acquired communications); *see also Jacobsen v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) ("Because Nevada Bell joined with the Washoe officials in the wiretapping, its failure to listen to the tapes should not insulate it from liability for the invasion of privacy it helped to occasion.") (citing *White v. Weiss*, 535 F.2d 1067, 1071 (8th Cir. 1976)).

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

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

---

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

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

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

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

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

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

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

---

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

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

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

c. Neither Title III nor FISA Authorizes Defendants' Conduct

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

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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