Privacy: Wiretap Act

From Internet Law Treatise

The Wiretap Act regulates the collection of actual content of wire and electronic communications. Codified in 18 U.S.C. §§ 2510-2522, the Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III". Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications.

Contents

In General

The Wiretap Act broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. See 18 U.S.C. § 2511(1). In general, these prohibitions bars third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.

However, when authorized by the Justice Department and signed by a United States District Court or Court of Appeals judge, a wiretap order permits law enforcement to intercept communications for up to thirty days. 18 U.S.C. §§ 2516(1), 2518(5). 18 U.S.C. §§ 2516-2518 imposes several formidable requirements that must be satisfied before investigators can obtain a Title III order. Most importantly, the application for the order must show probable cause to believe that the interception will reveal evidence of a predicate felony offense listed in § 2516. 18 U.S.C. § 2518(3)(a)-(b).

Exceptions

Provider Exception

18 U.S.C. § 2511(2)(a)(i) permits

> an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his

> employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

This exception grants providers the right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service." United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). However, it does not permit providers to conduct unlimited monitoring. See United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976) ("This authority of the telephone company to intercept and disclose wire communications is not unlimited."). Instead, the exception permits providers and their agents to conduct reasonable monitoring that balances the providers' needs to protect their rights and property with their subscribers' right to privacy in their communications. See United States v. Harvey, 540 F.2d 1345, 1351 (8th Cir. 1976) ("The federal courts . . . have construed the statute to impose a standard of reasonableness upon the investigating communication carrier."). Providers cannot use the rights or property exception to gather evidence of crime unrelated to their rights or property. United States v. Harvey, 540 F.2d 1345, 1352 (8th Cir. 1976).

Accessible to the Public Exception

18 U.S.C. § 2511(2)(g)(i) permits "any person" to intercept an electronic communication made through a system "that is configured so that . . . [the] communication is readily accessible to the general public." “[T]he legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards,” as opposed to publicly-accessible communications. See Konop, 302 F.3d at 875, citing S. Rep. No. 99-541, at 35-36, reprinted in 1986 U.S.C.C.A.N. 3555, 3599.

Key Definitions

Wire Communications

According to § 2510(1), "wire communication" means

> any aural transfer made in whole or in part though the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) 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 or foreign commerce.

The content of the communication must include the human voice. See § 2510(18) (defining "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and point of reception"). If a communication does not contain a genuine human voice, either alone or in a group conversation, then it cannot be a wire communication. See S. Rep. No. 99-541, at 12 (1986), reprinted in 1986 U.S.C.C.A.N. 3555; United States v. Torres, 751 F.2d 875, 885-86 (7th Cir. 1984) (concluding that "silent television surveillance" cannot lead to an interception of wire communications under Title III because no aural acquisition occurs). Prior to passage of the USA PATRIOT Act, the definition of "wire communication" in § 2510(1), unlike the definition of "electronic communication" in § 2510(12), explicitly included "any electronic storage of such communication."

Electronic Communications

18 U.S.C. § 2510(12) defines "electronic communication" as

> 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 does not include
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device . . . ; or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

"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)." H.R. Rep. No. 99-647, at 35 (1986).

In United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc), the First Circuit held "that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act."

U.S. v. Ropp, NO. CR 04-300-GAF (C.D. Cal. Oct. 8, 2004) held that the interception of keyboard keystrokes by a key logger is not a violation of the Wiretap Act because the transmission were not “electronic communications” within the meaning of the statute, which requires that the intercepted transmissions be “in interstate commerce.”

Interception

Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." The legislative history does not detail the meaning of “interception.” In discussing § 2510, however, the Senate Report on Title III focuses on the act of surveillance, and not the “aural acquisition” or hearing, of a conversation: “Paragraph (4) defines ‘intercept’ to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation.” S.Rep. No. 1097, 90th Cong., 2d Sess., reprinted in1968 U.S.Code Cong. & Admin.News 2112, 2178.

Communications are intercepted only if acquired contemporaneously with transmission. See *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 (D.N.J. 2001) (holding a key logger device on a personal computer will not intercept communications if it is configured such that keystrokes are not recorded when the computer's modem is in use).

"[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at that time." *U.S. v. Rodriguez,* 968 F.2d 130 (2d Cir. 1992); see also *In re State Police Litigation,* 888 F.Supp. 1235 (D.Conn. 1995) (interception occurs even without listening); *Jacobson v. Rose,* 592 F.2d 515, 522 (9th Cir. 1978) (Defendant's "failure to listen to the tapes should not insulate it from liability for the invasion of privacy it helped to occasion.”); *George v. Carusone,* 849 F. Supp. 159, 163 (D. Conn. 1994).

Hall v. Earthlink Network, Inc., 2005 U.S. App. Lexis 1230 (2d Cir. 2005) held that Earthlink’s continued reception of emails sent to plaintiff Hall’s account did not constitute an “interception” under the Wiretap Act

because it was part of Earthlnk's "ordinary course of business." See 18 U.S.C. § 2510 (http://www.law.cornell.edu/uscode/18/2510.html)(5)(a)).

Acquisition of the contents of stored electronic or wire communications is governed by § 2703(a) of the Stored Communications Act.

Chapter 7 - Privacy And Data Collection
Data Terminology · Statutory Protections · **The Wiretap Act (Title III)** · The Stored Communications Act · Government Agency Regulation · Searching and Seizing Computers · Key Privacy Cases · Industry Self-Regulation · International Issues