Chapter 2
Wiretap Act

The Wiretap Act, often referred to as "Title III," has as its dual purposes: "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153; *see also In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications"). Although the original act covered only wire and oral communications, Congress amended it in 1986 to include electronic communications. *See Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995) ("The principal purpose of the 1986 amendments to Title III was to extend to 'electronic communications' the same protections against unauthorized interceptions that Title III had been providing for 'oral' and 'wire' communications via common carrier transmissions"). The 1986 amendments make the Wiretap Act another option for prosecuting computer intrusions that include real-time capture of information.

Because this manual focuses on prosecution of criminal offenses, this chapter only addresses the first of the Wiretap Act's two purposes, protecting the privacy of communications. For more on law enforcement's access to information concerning communications, see U.S. Department of Justice, *Searching and Seizing Computers and Electronic Evidence in Criminal Investigations* (Office of Legal Education 2002). Also, in keeping with the manual's focus on computer crimes, this section highlights Title III's applicability in that context and does not address every type of case covered by the Act.[1]

[1] Section 2511(1)(b) applies only to certain interceptions of oral communications, i.e., communications that are "uttered by a person" and are not electronic communications. *See* 18 U.S.C. § 2510(2) (definition of "oral communication"). Accordingly, section 2511(1)(b) generally will not apply to network intrusions, which almost always involve electronic communications, and that section is not discussed here.

A. Intercepting a Communication: 18 U.S.C. § 2511(1)(a)

Summary

1. Intentional
2. interception (or endeavoring or procuring another to intercept)
3. of the contents
4. of a wire, oral or electronic communication
5. by use of a device

The core prohibition of the Wiretap Act is found at section 2511(1)(a), which prohibits any person from intentionally intercepting, or attempting to intercept, any wire, oral, or electronic communication." When the requirements of the defined terms are taken into account, a violation of this section has five elements. *See In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 18 (1st Cir. 2003).

Title 18, United States Code, Section 2511(1)(a) provides:

Except as otherwise specifically provided in this chapter any person who–

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication ….

shall be punished as provided in subsection (4).

1. Intentional

Since the 1986 amendments, in order to constitute a criminal violation, the interception of a covered communication must be "intentional"—deliberate and purposeful. *See United States v. Townsend*, 987 F.2d 927, 930 (2d Cir. 1993). In those amendments, Congress deliberately changed the mens rea requirement from "willfully" to "intentionally." *See* S. Rep. No. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577.

Although a defendant must have intended to intercept a covered communication, he or she need not have specifically intended to violate the Wiretap Act. In other words, a mistake of law is not a defense to a Wiretap Act charge. *See Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 178-79 (5th Cir. 2000); *Reynolds v. Spears*, 93 F.3d 428, 435-36 (8th Cir. 1996) (holding that reliance on incorrect advice from law enforcement officer is not a defense); *Williams v. Poulos*, 11 F.3d 271, 285 (1st Cir. 1993) (rejecting a good faith defense where defendant mistakenly believed his use and disclosure was authorized by the statute); *Thompson v. Dulaney*, 970 F.2d 744, 749 (10th Cir. 1992) (noting

that a "defendant may be presumed to know the law"); *Heggy v. Heggy*, 944 F.2d 1537, 1541-42 (10th Cir. 1991) (rejecting a "good faith" defense based upon a mistake of law).

2. Interception

The Wiretap Act defines an "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." 18 U.S.C. § 2510(4). This statutory definition does not explicitly require that the "acquisition" of the communication be *contemporaneous* with the transmission of the communication. However, a contemporaniety requirement is necessary to maintain the proper relationship between the Wiretap Act and the Electronic Communications Privacy Act's restrictions on access to stored communications.

Most courts addressing the potential overlap between the two acts have held that both wire and electronic communications are "intercepted" within the meaning of the Wiretap Act only when such communications are acquired contemporaneously with their transmission. An individual who obtains access to a stored copy of the communication does not "intercept" the communication. *See, e.g., Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 460-63 (5th Cir. 1994) (access to stored email communications); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-78 (9th Cir. 2002) (website); *Wesley College v. Pitts*, 974 F. Supp. 375, 384-90 (D. Del. 1997) (email); *United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990) (pager communications); *United States v. Reyes*, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (same); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (same); *United States v. Moriarty*, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (stored wire communications); *In re State Police Litigation*, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (same); *Payne v. Norwest Corp.*, 911 F. Supp. 1299, 1303 (D. Mont. 1995) (same), *aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997) (same).

A divided panel of the First Circuit took this line of reasoning to an extreme in an opinion later withdrawn by the First Circuit after rehearing the case en banc. *See United States v. Councilman*, 373 F.3d 197 (1st Cir.), *rehearing en banc granted and opinion withdrawn*, 385 F.3d 793 (1st Cir. 2004), *reversed on rehearing en banc*, 418 F.3d 67 (1st Cir. 2005). In *Councilman*, a divided panel of the First Circuit affirmed the dismissal of the indictment for conspiracy to wiretap electronic mail messages. 373 F.3d at 197. The defendant was charged

with acquiring the email messages contemporaneously with their transmission. The indictment alleged that before email messages were ultimately delivered to customers, the defendant's software program made copies of the messages from the servers that were set up to deliver the messages. Two of the three judges agreed with dicta from earlier cases that such email messages acquired from a computer's random access memory (RAM) or hard disk are outside the scope of the Wiretap Act. *Id.* On rehearing en banc, the First Circuit reversed the panel decision, holding that email in electronic storage can be intercepted electronic communications when acquired contemporaneously with their transmission. 418 F.3d at 67.

Notwithstanding the ultimate reversal on the panel's decision in *Councilman*, any prosecutor outside the First Circuit confronting an interception involving acquisition of information from any type of computer memory should anticipate the possibility of a *Councilman* defense. This may apply to prosecutions of spyware users and manufacturers, intruders using packet sniffers, or persons improperly cloning email accounts. Defendants accused of these types of interceptions may argue that the communications they acquired were "in electronic storage" at the time of acquisition, and therefore were not intercepted under Title III.

Even with the possibility of a *Councilman*-type defense, prosecutors should continue to charge violations of section 2511(1)(a) when an individual acquires the contents of a communication contemporaneously with its transmission or in a manner that is effectively contemporaneous with transmission. If a *Councilman*-type argument appears to apply to a prosecution, prosecutors are encouraged to contact CCIPS at (202) 514-1026. Prosecutors may also consider charging violation of section 2701(a) (access to communications residing in an electronic communication service provider facility) for unread email messages or section 1030(a)(2)(C) (unauthorized access to and obtaining information from protected computers) in addition to the Wiretap Act.

3. Contents of a Communication

To be an interception, the acquisition must be of the *contents* of the communication. 18 U.S.C. § 2510(4). "'[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Congress amended the definition in 1986 to "distinguish[] between the substance, purport or meaning of the communication and the

existence of the communication or transactional records about it." S. Rep. No. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.

Some types of information concerning network communications, such as full-path URLs, may raise arguments about whether they contain content. We encourage prosecutors who have questions about whether a particular type of information constitutes "contents" under the Wiretap Act to contact CCIPS for assistance at (202) 514-1026.

4. Wire, Oral, or Electronic Communication

The Wiretap Act prohibits the interception of "any wire, oral or electronic communication." 18 U.S.C. § 2511(1)(a). Each of the three types of communications covered by the Wiretap Act is separately defined by the statute. *See* 18 U.S.C. § 2510(1) (wire), (2) (oral), & (12) (electronic). Typically, network communications that do not contain the human voice will fall into the broad catch-all category of "electronic communications." *See* S. Rep. 99-541, at 14 ("As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice").

An "electronic communication" is "any transfer ... transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). In the context of network crimes, some defendants may attempt to convince courts to parse an intercepted communication into separate "transfers" in order to have their conduct excluded from this definition of an "electronic communication."

For instance, a defendant has claimed that his device that acquired transfers between a keyboard and a computer did not acquire any electronic communications. *United States v. Ropp,* 347 F. Supp. 2d 831 (C.D. Cal. 2004). In *Ropp*, the defendant placed a piece of hardware between the victim's computer and her keyboard that recorded the signals transmitted between the two. *Id.* The court dismissed the indictment charging a violation of section 2511 because it found that the communications that were acquired were not "electronic communications" within the meaning of the statute. *Id.* The court concluded that "the communications in question involved preparation of emails and other communications, but were not themselves emails or any other communication at the time of the interception." *Id.* at 835 n.1. Because the court found that the typing was a communication "with [the victim's] own computer," it reasoned

that "[a]t the time of interception, [the communications] no more affect[] interstate commerce than a letter, placed in a stamped envelope, that has not yet been mailed." *Id*.

Notwithstanding the *Ropp* decision, prosecutors should pursue cases involving interceptions occurring on computers or internal networks that affect interstate commerce. For example, if an individual installs malicious software on the victim's computer that makes a surreptitious copy every time an email is sent, or captures such messages as they move on the local area network on their way to their ultimate destination half way around the world, such cases can be prosecuted under section 2511.

The text of section 2511 and the statute's legislative history support this interpretation. A transfer should include all transmission of the communication from the originator to the recipient. First, the plain text of the definition of "electronic communication" is incompatible with such a piecemeal approach. The definition explicitly contemplates that a "transfer" may be transmitted by a system "in whole or in part." If "transfer" were meant to refer to each relay between components on a communication's journey from originator to recipient, no system could be said to transmit a transfer "in part." In addition, the legislative history of the 1986 amendments that added the term "electronic communication" provides some useful explanation. The House Report explicitly states that "[t]o the extent that electronic and wire communications passing through [customer equipment] affect interstate commerce, the Committee intends that those communications be protected under section 2511." H.R. Rep. No. 99-647, at 33. Similarly, the Senate Report discusses the inclusion of communications on private networks and intracompany communications systems. *See* S. Rep. No. 99-541, at 12, *reprinted in* 1968 U.S.C.C.A.N. 3555, 3566. In these discussions, Congress explicitly rejected the premise that acquiring a communication on the customer's own equipment would take it out of the protections of the Wiretap Act. *See* H.R. Rep. No. 99-647, at 33 (discussing interceptions occurring at customer's premises on customer equipment connected to public or private communications networks and making clear that such interceptions violate the Act).

5. Use of a Device

Finally, to be an interception under the Act, the acquisition must be by use of an "[e]lectronic, mechanical or other device." 18 U.S.C. § 2510(4). Generally, "'electronic, mechanical or other device' means any device or apparatus which

can be used to intercept a wire, oral, or electronic communication" subject to two specific exceptions. 18 U.S.C. § 2510(5).

The little existing case law on what constitutes a device focuses on the exceptions to the rule, rather than on what actually qualifies as a device. *See, e.g., Adams v. Sumner*, 39 F.3d 933 (9th Cir. 1994). In a typical network crime, the device used could be the computer that is used to intercept the communication or a software program running on such a computer. Each appears to satisfy the statutory requirements. *See* 18 U.S.C. § 2510(5).

The definition of device explicitly excludes (1) equipment used in the ordinary course of service (e.g., a telephone used for telephone service) and (2) hearing aids used to "correct subnormal hearing to not better than normal." *Id.* In addition, the "extension telephone" exception excludes:

> any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

18 U.S.C. § 2510(5)(a). Congress intended this exception to have a fairly narrow application: the exception was designed to permit businesses to monitor by way of an "extension telephone" the performance of their employees who spoke on the phone to customers. The "extension telephone" exception makes clear that when a phone company furnishes an employer with an extension telephone for a legitimate work-related purpose, the employer's monitoring of employees using the extension phone for legitimate work-related purposes does not violate Title III. *See Briggs v. American Air Filter Co.*, 630 F.2d 414, 418 (5th Cir. 1980) (reviewing legislative history of Title III); *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (applying exception to permit monitoring of sales representatives); *James v. Newspaper Agency Corp*. 591 F.2d 579, 581 (10th Cir. 1979) (applying exception to permit monitoring of newspaper employees' conversations with customers).

The case law interpreting the extension telephone exception is notably erratic, largely owing to the ambiguity of the phrase "ordinary course of business." Some courts have interpreted "ordinary course of business" broadly to mean "within the scope of a person's legitimate concern," and have applied the extension telephone exception to contexts such as intrafamily disputes. *See, e.g., Simpson v. Simpson*, 490 F.2d 803, 809 (5th Cir. 1974) (holding that husband did not violate Title III by recording wife's phone calls); *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977) (holding that husband did not violate Title III in recording wife's conversations with their daughter in his custody). Other courts have rejected this broad reading, and have implicitly or explicitly excluded surreptitious activity from conduct within the "ordinary course of business." *See Kempf v. Kempf*, 868 F.2d 970, 973 (8th Cir. 1989) (holding that Title III prohibits all wiretapping activities unless specifically excepted and that the Act does not have an express exception for interspousal wiretapping); *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974) ("We hold as a matter of law that a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business"); *Pritchard v. Pritchard*, 732 F.2d 372, 374 (4th Cir. 1984) (rejecting view that § 2510(5)(a) exempts interspousal wiretapping from Title III liability). Some of the courts that have embraced the narrower construction of the extension telephone exception have stressed that it permits only limited work-related monitoring by employers. *See, e.g., Deal v. Spears*, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that employer monitoring of employee was not authorized by the extension telephone exception in part because the scope of the interception was broader than that normally required in the ordinary course of business).

On top of the ambiguities concerning the contours of this carve-out from the definition of device, it is not at all clear that this exception would transfer to the network crime context. While computers may qualify as equipment or facilities, whether "telephone or telegraph" modifies all three types of objects, i.e., "instrument, equipment or facility," or only instruments, is not yet settled.

Moreover, the exception in section 2510(5)(a)(ii) that permits the use of "any telephone or telegraph instrument, equipment or facility, or any component thereof" by "an investigative or law enforcement officer in the ordinary course of his duties" is a common source of confusion. This language does *not* permit agents to intercept the private communications of the targets

of a criminal investigation on the theory that a law enforcement agent may need to intercept communications "in the ordinary course of his duties." As Chief Judge Posner explained:

> Investigation is within the ordinary course of law enforcement, so if "ordinary" were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, "ordinary" should not be read so broadly; it is more reasonably interpreted to refer to routine non investigative recording of telephone conversations .... Such recording will rarely be very invasive of privacy, and for a reason that does after all bring the ordinary-course exclusion rather close to the consent exclusion: what is ordinary is apt to be known; it imports implicit notice.

Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999). For example, routine taping of all telephone calls made to and from a police station may fall within this law enforcement exception, but non-routine taping designed to target a particular suspect ordinarily would not. *See id.*; *accord United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002) (concluding that routine recording of calls made from prison falls within law enforcement exception); *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (same).

B. Disclosing an Intercepted Communication: 18 U.S.C. § 2511(1)(c)

Summary

1. Intentional disclosure
2. of Illegally intercepted communication
3. knowledge or reason to know the intercept was illegal

The Wiretap Act prohibits not only the interception of communications, but also the intentional disclosure of communications that are known to have been illegally intercepted. 18 U.S.C. § 2511(1)(c).

Title 18, United States Code, Section 2511(1)(c) provides:

Except as otherwise specifically provided in this chapter any person who–

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception

of a wire, oral, or electronic communication in violation of this subsection
....
shall be punished as provided in subsection (4).

1. Intentional Disclosure

While the statute unquestionably covers the disclosure of the actual contents of a communication, courts have interpreted the disclosure prohibition more broadly. *See Deal v. Spears*, 780 F. Supp. 618, 624 (W.D. Ark. 1991) (finding liability for disclosure when only the "nature" of the communications was disclosed), *aff'd*, 980 F.2d 1153 (8th Cir. 1992). However, disclosure of the mere fact that an illegal interception took place does not violate the prohibition on disclosure of the contents of intercepted communications. *See Fultz v. Gilliam*, 942 F.2d 396, 403 (6th Cir. 1991). In addition, disclosure of the contents of an intercepted communication that has already become "public information" or "common knowledge" is not prohibited. *See* S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2181.

2. Illegal Interception of Communication

Generally, there can be no illegal disclosure of an illegally intercepted communication without an underlying violation of section 2511(1)(a). Although the defendant need not be the individual who intercepted the communication, in most cases the prosecution must prove that someone intercepted a covered communication in violation of section 2511(1)(a), covered above.

The Senate Report suggests an exception to the general rule that section 2511(1)(a) must have been violated. If a communication is intercepted, but the interception does not violate section 2511(1)(a) only because the interception was not intentional, the Senate Report states that use or disclosure of the communication would still violate the Act. *See* S. Rep. No. 99-541, at 25 (1986), *reprinted in* 1968 U.S.C.C.A.N. 3555, 3579.

3. Knowledge of the Illegal Interception

The prosecution must also prove that the disclosing individual knew or had reason to know that the "information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." 18 U.S.C. § 2511(1)(c). As with section 2511(1)(a), mistake of law is not a defense in that the prosecution need show only that the defendant knew the relevant facts, not that the defendant knew that the interception was in fact

unlawful. *See United States v. Wuliger*, 981 F.2d 1497, 1501 (6th Cir. 1992); *see also Williams v. Poulos*, 11 F.3d 271, 284-85 (1st Cir. 1993). However, a prosecutor should be prepared to defeat any claim that the defendant was mistaken about any fact that would have authorized the interception. *See id*.

4. First Amendment Limitation

Although the prohibition on disclosure is broad, the Supreme Court has narrowed the scope of section 2511(1)(c) in one very particular set of circumstances. *Bartnicki v. Vopper*, 532 U.S. 514 (2001). In *Bartnicki*, several news organizations received a tape recording of a telephone conversation that they should have known was illegally intercepted. The majority held that the First Amendment prevents application of the statute to a disclosure of information of public concern by a third party not involved in the interception. The case involved a question of immunity from statutorily imposed civil liability, but the same First Amendment principles should apply to criminal liability as well.

Although *Bartnicki* demonstrates that the First Amendment does limit the applicability of section 2511(1)(c), the concurring opinions suggest that those limits are very narrow. For instance, a defendant will not be exempt from prosecution merely because he discloses information of interest to the public. Two of the six Justices in the majority in *Bartnicki* filed a separate concurring opinion that makes clear that a majority of the Court rejects a "public interest" exception to the disclosure provisions of the Wiretap Act. *See Bartnicki*, 532 U.S. at 540 (Breyer, J., concurring).

In concurring with the result in *Bartnicki*, Justice Breyer, with whom Justice O'Connor joined, agreed that privacy interests protected by section 2511(1)(c) must be balanced against media freedom embodied in the First Amendment. Justice Breyer wrote separately, however, to emphasize several facts he found particularly relevant in the case presented. In particular, he found that "the speakers had little or no *legitimate* interest in maintaining the privacy of the particular conversation." *Id.* at 539 (emphasis in original). Justice Breyer based this conclusion on three factors: (1) the content of the communication, (2) the public status of the speaker, and (3) the method by which the communication was transmitted. According to Justice Breyer, the conversation intercepted involved threats to harm others, which the law has traditionally treated as not entitled to remain private. Moreover, Justice Breyer concluded that the speakers were "limited public figures." *Id.* Finally, the speakers chose to communicate in what Justice Breyer viewed as an insecure method, via an unencrypted cellular

telephone. "Eavesdropping on ordinary cellular phone conversations in the street (which many callers seem to tolerate) is a very different matter from eavesdropping on encrypted cellular phone conversations or those carried on in the bedroom." *Id.* at 541.

Although prosecutors should be aware of the First Amendment limits outlined in *Bartnicki*, the First Amendment will probably be implicated very rarely. In *Bartnicki*, the Supreme Court explicitly did not address cases where (1) the disclosing party participated in any illegality in obtaining the information, or (2) the disclosure is of "trade secrets or domestic gossip or other information of purely private concern." *Id.* at 528, 533. In addition, the limits identified in *Bartnicki* explicitly do not apply to prosecutions under section 2511(1)(d) for using an illegally intercepted communication, which the Supreme Court expressly characterized as a regulation of conduct, not pure speech. *See id.* at 526-27.

Finally, note that the First Amendment does not create a general defense to Wiretap Act violations for media. If this was not obvious from the care with which the Supreme Court limited the exception in *Bartnicki*, several courts have explicitly so held. *See Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000); *Sussman v. ABC, Inc.*, 186 F.3d 1200 (9th Cir. 1999); *Vasquez-Santos v. El Mundo Broad. Corp.*, 219 F. Supp. 2d 221, 228 (D.P.R. 2002) (rejecting a blanket exemption from Wiretap Act liability for interceptions that occur for a tortious purpose during a media investigation).

C. Using an Intercepted Communication: 18 U.S.C. § 2511(1)(d)

Summary

1. Illegal interception of communication
2. knowledge or reason to know the intercept was illegal
3. use of the contents

Like a violation of subsection (1)(c), a charge under section 2511(1)(d) has three elements. The first two elements are the same as in section 2511(1)(c) and present the same issues discussed above.

Title 18, United States Code, Section 2511(1)(d) provides:

Except as otherwise specifically provided in this chapter any person who–

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that

the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection ….

shall be punished as provided in subsection (4).

The third element is different. "Use of the contents" of the intercepted communication is intended to be extremely broad. However, "use" does require some "active employment of the contents of the illegally intercepted communication for some purpose." *Peavy v. Harman*, 37 F. Supp. 2d 495, 513 (N.D. Tex. 1999), *aff'd in part and reversed in part*, 221 F.3d 258 (5th Cir. 2000). Accordingly, "use" does not include mere listening to intercepted conversations. *See, e.g., Dorris v. Absher*, 179 F.3d 420, 426 (6th Cir. 1999); *Reynolds v. Spears*, 93 F.3d 428, 432-33 (8th Cir. 1996); *Fields v. Atchison, Topeka and Santa Fe Ry. Co.*, 985 F. Supp. 1308 (D. Kan. 1997), *withdrawn in part*, 5 F. Supp. 2d (D. Kan 1998) ; *but see Thompson v. Dulaney*, 838 F. Supp. 1535, 1547 (D. Utah 1993) (finding listening was a use).

Because "use" is extremely broad, it may reach many of the cases that would otherwise be difficult to prosecute due to *Bartnicki*. For instance, a court has held that threatened disclosure in order to influence another is a "use." *See Leach v. Bryam*, 68 F. Supp. 2d 1072 (D. Minn. 1999). In the network context, other uses might include the use of intercepted passwords to gain access to other computers or use of intercepted confidential business information for commercial advantage.

D. Statutory Exceptions

The breadth of the Wiretap Act's general prohibitions against intercepting oral, wire, and electronic communications makes the statutory exceptions found in subsection 2511(2) particularly important. The exceptions that are particularly relevant in the context of network crimes are discussed below. A prosecutor should consider whether these exceptions apply in his or her case before undertaking a prosecution under the Wiretap Act. The applicability of these exceptions will be fact-dependent.

1. Provider Exception

The Wiretap Act provides that:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of a 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.

18 U.S.C. § 2511(2)(a)(i).

The "rights or property of the provider" clause of subsection 2511(2)(a)(i) exempts providers from criminal liability for "intercept[ing] and monitor[ing 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). For example, employees of a cellular phone company may intercept communications from an illegally "cloned" cell phone in the course of locating its source. *See United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997). The rights or property clause also permits providers to monitor misuse of a system in order to protect the system from damage or invasions of privacy. For example, system administrators can track intruders within their networks in order to prevent further damage. *See United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (concluding that need to monitor misuse of computer system justified interception of electronic communications pursuant to subsection 2511(2)(a)(i)).

The rights and property clause of the provider exception does not permit providers to conduct unlimited monitoring. *See United States v. Auler*, 539 F.2d 642, 646 (7th Cir. 1976). The exception permits providers and their agents to conduct reasonable monitoring that balances the providers' need 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.").

Thus, providers investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under subsection 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure to minimize the interception and disclosure of private communications unrelated

to the investigation. *See, e.g., United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975) (concluding that phone company investigating use of illegal devices designed to steal long-distance service acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every illegal conversation but did not intercept legitimately authorized communications). In particular, there must be a "substantial nexus" between the monitoring and the threat to the provider's rights or property. *United States v. McLaren*, 957 F. Supp. 215, 219 (M.D. Fla. 1997); *see Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967) (interpreting Title III's predecessor statute, 47 U.S.C. § 605, and holding impermissible provider monitoring to convict blue box user of interstate transmission of wagering information).

Where a service provider supplies a communication to law enforcement that was intercepted pursuant to the rights and property exception, courts have scrutinized whether the service provider was acting as an agent of the government when intercepting communications. For example, in *McClelland v. McGrath*, 31 F. Supp. 2d 616 (N.D. Ill. 1998), a user of a cloned cellular telephone sued police officers for allegedly violating the Wiretap Act by asking telephone company to intercept his calls in connection with a kidnapping investigation. In dismissing the defendant's motion for summary judgment, the District Court found that a genuine issue of fact existed as to whether the phone company was impermissibly acting as the government's agent when it intercepted the plaintiff's call. *Id.* at 618. The Court opined that the officers were not free to ask or direct the service provider to intercept any phone calls or disclose their contents without complying with the judicial authorization provisions of the Wiretap Act, regardless of whether the service provider was entitled to intercept those calls on its own initiative. *Id.*; s*ee also United States v. McLaren*, 957 F. Supp. at 215. If the provider's interception of communications pursuant to the rights and property clause preceded law enforcement's involvement in the matter, no agency existed at the time of interception and the provider exception applies. *See United States v. Pervaz*, 118 F.3d at 5-6.

The "necessary … to the rendition of his service" clause of subsection 2511(2)(a)(i) permits providers to intercept, use, or disclose communications in the ordinary course of business when interception is unavoidable. *See United States v. New York Tel. Co.*, 434 U.S. 159, 168 n.13 (1977) (noting that § 2511(2)(a)(i) "excludes all normal telephone company business practices from the prohibition of [Title III]"). For example, a switchboard operator may briefly overhear conversations when connecting calls. *See, e.g., United States v. Savage*,

564 F.2d 728, 731-32 (5th Cir. 1977); *Adams v. Sumner*, 39 F.3d 933, 935 (9th Cir. 1994). Similarly, repairmen may overhear snippets of conversations when tapping phone lines in the course of repairs. *See United States v. Ross*, 713 F.2d 389, 392 (8th Cir. 1983). Although the "necessary incident to the rendition of his service" language has not been interpreted in the context of electronic communications, these cases concerning wire communications suggest that this phrase would likewise permit a system administrator to intercept communications in the course of repairing or maintaining a computer network.

For a more thorough discussion of this exception, see U.S. Department of Justice, *Searching and Seizing Computers and Electronic Evidence* (Office of Legal Education 2002), section IV.D.3.c.

2. Consent of a Party

The consent exceptions under paragraphs 2511(2)(c) and (d) are perhaps the most frequently cited exceptions to the Wiretap Act's general prohibition on intercepting communications. Section 2511(2)(c) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

Under the Wiretap Act, government employees are not considered to be "acting under color of law" merely because they are government employees. *See Thomas v. Pearl*, 998 F.2d 447, 451 (7th Cir. 1993). Whether a government employee is acting under color of law under the wiretap statute depends on whether the individual was acting under the government's direction when conducting the interception. *See United States v. Andreas, 216 F.3d 645, 660 (7th Cir. 2000); United States v. Craig*, 573 F.2d 455, 476 (7th Cir, 1977); *see also Obron Atlantic Corp. v. Barr*, 990 F.2d 861, 864 (6th Cir. 1993); *United States v. Tousant*, 619 F.2d 810, 813 (9th Cir. 1980). The fact that a party to whom consent is provided is secretly cooperating with the government does not vitiate consent under paragraph 2511(2)(c). *United States v. Shields*, 675 F.2d 1152, 1156-57 (11th Cir. 1982).

The second exception provides that

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication

> where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d); *see also Payne v. Norwest Corp.*, 911 F. Supp. 1299, 1303 (D. Mont. 1995) (applying exception absent evidence of criminal or tortious purpose for recording of conversations), *rev'd on other grounds*, 113 F.3d 1079 (9th Cir. 1997). A criminal or tortious purpose must be a purpose other than merely to intercept the communication to which the individual is a party. *See Roberts v. Americable Int'l, Inc.*, 883 F. Supp. 499, 503 (E.D. Cal. 1995).

In the context of network communications, it may not always be clear who is a party to a communication capable of furnishing consent to intercept. The Senate report for the Wiretap Act defined "party" as "the person actually participating in the communication." S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182. Generally, a provider does not *participate* in the communications of its subscribers, but rather merely *transmits* them. Therefore, a service provider generally should not be considered a party to communications occurring on its system. Indeed, if service providers were capable of consenting to interception of communications as parties to communications occurring on their own systems, the exception that protects the rights and properties of service providers would be unnecessary. *See* 18 U.S.C. § 2511(2)(a)(i).

The courts have provided additional guidance about who constitutes a "party." It is clear, for example, that individuals are parties to a communication when statements are directed at them, even if they do not respond, *United States v. Pasha*, 332 F.2d 193 (7th Cir. 1964) (officer who answered phone during execution of warrant on gambling establishment was party to statements placing bets), or if they lie about their identity. *United States v. Campagnuolo*, 592 F.2d 852, 863 (5th Cir. 1979) (officer who answered phone in gambling establishment and pretended to be defendant was a party). At least one court appears to have taken a broader approach, holding that someone whose presence is known to other communicants may be a party, even if the communicants do not address her, nor she them. *See, e.g., United States v. Tzakis*, 736 F.2d 867, 871-72 (2d Cir. 1984). In appropriate cases, however, prosecutors should consider charging an individual who overhears or records conversations between

others who do not know that he is present, as such a person is not a party to the communication.

Consent under subsections 2511(2)(c) and (d) may be explicit or implied. *See United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987). The key to establishing implied consent in most cases is showing that the consenting party received actual notice of the monitoring and used the monitored system regardless. *See United States v. Workman*, 80 F.3d 688, 693 (2d Cir. 1996); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) ("[I]mplied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.") (internal quotation marks omitted); *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) ("Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception.") (internal quotation marks omitted). However, consent must be "actual" rather than "constructive." *See In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 19-20 (1st Cir. 2003) (*citing* cases). Proof of notice to the party generally supports the conclusion that the party knew of the monitoring. *See Workman*, 80 F.3d. at 693; *but see Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992) (finding lack of consent despite notice of possibility of monitoring). Absent proof of notice, it must be "convincingly" shown that the party knew about the interception based on surrounding circumstances in order to support a finding of implied consent. *See United States v. Lanoue*, 71 F.3d 966, 981 (1st Cir. 1995).

A network banner alerting the user that communications on the network are monitored and intercepted may be used to demonstrate that a user furnished consent to intercept communications on that network. *United States v. Angevine*, 281 F.3d 1130, 1133 (10th Cir. 2002); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

3. Computer Trespasser Exception

Section 2511(2)(i) allows victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Section 2511(2)(i) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

Under paragraph 2511(2)(i), law enforcement—or a private party acting at the direction of law enforcement—may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, the four requirements found in section 2511(2)(i)(I)-(IV) must be met. Interceptions conducted by private parties not acting in concert with law enforcement are not permitted under the computer trespasser exception.

Under the definition of "computer trespasser" found in section 2510(21)(A), a trespasser includes any person who accesses a protected computer (as defined in 18 U.S.C. § 1030) without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the computer." 18 U.S.C. § 2510(21)(B). This provision, while harmless, was unnecessary, since a contractual relationship is just one way to show authority to access a network. For example, certain Internet service providers do not allow their customers to send bulk unsolicited emails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers—both because their access of the network is authorized and because they have an existing contractual relationship with the provider.

E. Defenses

In addition to the statutory exceptions provided by section 2511, section 2520 (which generally deals with recovery of civil damages) also includes several defenses against any civil *or criminal* action brought under the Wiretap Act. The "good faith" defenses in section 2520 prevent prosecution of a defendant who relied in good faith on listed types of lawful process (e.g., warrants, court orders, grand jury subpoenas) or an emergency request (under 18 U.S.C. § 2518(7)). 18 U.S.C. § 2520(d)(1), (2). These defenses are most commonly applicable to law enforcement officers executing legal process and service providers complying with legal process, even if the process later turns out to be deficient in some manner. Similarly, section 2520(d)(3) protects a person acting under color of law when that person believes in good faith that interception is warranted by the computer trespasser exception. *See* 18 U.S.C. § 2520(d)(3) (creating a defense for good faith reliance on a good faith determination that, *inter alia*, section 2511(2)(i) permitted the interception).

The final subsection of section 2520(d) provides that "good faith reliance" on "a good faith determination that section 2511(3) ... permitted the conduct complained of" is a "complete defense." 18 U.S.C. § 2520(d)(3). Section 2511(3) permits a provider of electronic communication service to the public to divulge the contents of communications under certain enumerated circumstances.

The defenses provided under subsection 2520(d) are affirmative defenses, *United States v. Councilman*, 418 F.3d 67, 89 (1st Cir. 2005), thus placing the burden of proof on the defendant. Whereas a mistake of law is not a defense for non-providers, *see* section B.1 of this chapter on page 64, some good faith mistakes of law are a defense for providers of electronic communication service to the public under subsection 2520(d)(3).

F. Statutory Penalties

A Wiretap Act violation is a Class D felony; the maximum authorized penalties for a violation of section 2511(1) of the Wiretap Act are imprisonment of not more than five years and a fine under Title 18. *See* 18 U.S.C. §§ 2511(4)(a) (setting penalties), 3559(a)(4) (classifying sentence). Authorized fines are typically not more than $250,000 for individuals or $500,000 for an organization, unless there is a substantial loss. *See* 18 U.S.C. § 3571 (setting fines for felonies). Generally applicable special assessments

and terms of supervised release also apply. *See* 18 U.S.C. § 3013(a)(2) (setting special assessments for felonies at $100 for individuals; $400 for persons other than individuals), 18 U.S.C. § 3583(b)(2) (allowing imposition of a term of supervised release not more than three years for a Class D felony).

For a discussion of the Sentencing Guidelines applicable to Wiretap Act violations, please see Chapter 5.