

## AN OVERVIEW OF NHRSA 570-A IN THE DOMESTIC CONTEXT

Michael J. Iacopino  
Brennan Caron Lenehan & Iacopino  
85 Brook Street  
Manchester, N.H. 03104

## **AN OVERVIEW OF NHRSA 570-A IN THE DOMESTIC CONTEXT**

*Our whole lives are lived in a tangle of telling, not telling, misleading, allowing to know, concealing, eavesdropping and collusion. When Washington said he could not tell a lie, his father must have answered, "You had better learn."*

Germaine Greer (1939 - )

### **Introduction**

The purpose of this article is to provide an overview of state law governing electronic eavesdropping and to analyze its relevance in the context of domestic relations. The article does not address the statutes and/or constitutional concerns which govern law enforcement officials and other government authorities; nor, does it address the laws and regulations which govern telephone service and electronic communications providers.

Husbands and wives can be notorious snoops. The intimacy of a marriage (or other close) relationship puts domestic partners into close proximity with each other and each other's personal effects. A family's livelihood usually depends upon the interpersonal and business relationships of one or both partners. In a family relationship eavesdropping is commonplace and oftentimes necessary to the successful functioning of the family unit. However, when domestic bliss hits a bump in the road it is not uncommon to find partners secretly intercepting telephone conversations, e-mail or other communications that might prove an adulterous relationship or the existence of hidden assets or business relationships. It is usually under these circumstances that the practitioner must become familiar with the law of electronic eavesdropping in both the civil and criminal context as well the evidentiary issues which will arise.

Electronic eavesdropping is the subject of both state and federal statutes. In

New Hampshire, R.S.A. 570-A, entitled, “Wiretapping and Eavesdropping,” provides state regulation of such conduct. Federally, the Federal Wiretap Act, 18 U.S.C. § 2510, *et. seq.*, and the Stored Communications Act, 18 U.S.C. § 2701, *et. seq.*, govern electronic eavesdropping and interception of electronic communications. Although the state statute is said to resemble the federal statute, *see, State v. Telles*, 139 NH 344,346 (1995), they do have some different provisions. The state statute has been interpreted to provide more stringent protection of individual privacy rights than its federal counterpart. *State v. Kepple*, \_\_\_\_ N.H. \_\_\_\_, 866 A.2d 959, 961 (2005)

From a criminal perspective, prosecutions under the state statute due to domestic eavesdropping do occur, albeit, infrequently. Prosecutions by federal authorities in the domestic context are rare. The United States Department of Justice has recognized various levels of severity concerning wiretapping violations. In the United States Attorney Manual the DOJ has relegated “domestic eavesdropping “ offenses to the category of “lowest priority:”

Domestic relations violations which do not involve a professional interceptor are the lowest priority cases for federal prosecution. Although local prosecution is normally preferable, when local prosecutors are unwilling to pursue the case, resort to federal prosecution may be appropriate. Nevertheless, violations of this type will sometimes prove to be of insufficient magnitude to warrant either federal or state prosecution. In such cases, other measures may prove sufficient, for example, a civil suit for damages (18 U.S.C. §§ 2520), suppression of evidence (18 U.S.C. §§ 2515), or forfeiture of the wiretapping or eavesdropping paraphernalia (18 U.S.C. §§ 2513).

United States Attorney Manual §9-60.202<sup>1</sup>. Due to the broader scope of the state statute and the federal DOJ’s “low priority” policy this article will only address the state

---

<sup>1</sup>This section of the United States’ Attorney Manual is reproduced in the appendix.

wiretapping statute, RSA 570-A.

### **RSA 570-A “It Takes Two to Tango.”**

The primary differences between the New Hampshire statute and the federal statute revolve around the issue of consent. The federal statute and many other state statutes permit recording and/or interception of telecommunications if one of the parties to the conversation consents to such interception and/or recording. Thus, in the standard domestic context where one family member records their own conversation with another family member there is no violation. New Hampshire, on the other hand, is considered to be a “two party” consent state. In other words, it is lawful to intercept or record a conversation only if both parties (or all parties if there are more than two) have consented to the interception and /or recording of the conversation. It is important to understand the basic elements of the state statute. R.S.A. 570-A criminalizes unauthorized “interception” of any “oral communication” or “telecommunication” without the “consent” of all parties. See, R.S.A. 570-A:2. The disclosure or use of such intercepted communications is also illegal. RSA 570-A:2, I, (c)and (d). The statute also criminalizes the possession, manufacture, distribution and advertising of devices which are “primarily useful for the purpose of surreptitious interception of telecommunications or oral communications.” See, R.S.A. 570-A:3, I (a).

### **The Elements of “Interception Offenses” Under RSA 570-A**

Under RSA 570-A:2, a person is guilty of a Class B Felony<sup>2</sup> if she:

---

<sup>2</sup>A Class B Felony is punishable by a maximum sentence to the New Hampshire State Prison of not more than seven (7) nor less than three and one half (3 1/2) years and a fine of Four Thousand Dollars (\$4,000.00). See, RSA 651:2, II (b); RSA 651:2, IV.

1. Willfully intercepts any telecommunication or oral communication. See RSA 570-A:2, I<sup>3</sup>.

2. Wilfully uses any electronic, mechanical, or other device to intercept any oral communication when:

(A) Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in telecommunication, or

(B) Such device transmits communications by radio, or interferes with the transmission of such communication, or

(C) Such use<sup>4</sup>: (A) takes place on premises of any business or other commercial establishment, or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment. See RSA 570-A:2, I, (b).

(3) Wilfully discloses<sup>5</sup>, to any other person the contents of any telecommunication or oral communication, knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in violation of RSA 570-A:2, I. See, RSA 570-A: 2, I, (c).

(4) Willfully uses, or endeavors to use, the contents of any telecommunication or oral communication, knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in

---

<sup>3</sup>The statute also prohibits endeavors to intercept, and procuring another person to intercept or endeavor to intercept. See, RSA 570-A:2, I, (a).

<sup>4</sup> The statute also prohibits “endeavors to use.” See, RSA 570-A:2, I, (b).

<sup>5</sup> The statute also prohibits “endeavors to disclose.” See, RSA 570-A: 2, I, (c).

violation of RSA 570-A:2, I. See, RSA 570-A:2, I, (d).

The state statute, RSA 570-A:2, I-a, also creates a misdemeanor offense when a person knowingly intercepts a telecommunication or oral communication when the person is a party to the communication or obtains the consent of one party but does not have the approval of the attorney general under RSA 570-A:2, II, (d)<sup>6</sup>.

### **The Elements of “Possession” Offenses Under RSA 570-A:3.**

The state statute prohibits the “manufacturing, assembling, possession, or sale” of an “electronic, mechanical or other device” which the person “knows or has reason to know” that the “design of such device renders it primarily useful for the purpose of the surreptitious interception of telecommunications or oral communications.” See, RSA 570-A:3, I, (a). Similarly the statute prohibits the advertising of such devices or the advertising promotion of any device for the surreptitious interception of telecommunications or oral communications.” See, RSA 570-A:3, I, (b).

### **The Purpose of RSA 570-A**

Since its inception the statute has been recognized as a method “to maintain a proper balance between the duty of the State to protect the public and the individual's right of privacy and free expression.” State v. Lee, 113 NH 313, 316 (1973.) The Court has also recognized that the state statute, RSA 570-A, is “more stringent than its federal counterpart, providing more protection for the individual's right to privacy.” State v. Kepple, \_\_\_\_ N.H. \_\_\_\_, 866 A.2d 959, 961 (2005.) The statute, in barring the “use”

---

<sup>6</sup>RSA 570-A:2, II, (d) permits a law enforcement official to lawfully intercept communications when he is a party to the communication or has the consent of one party and the approval of the attorney general or her designee.

of intercepted communications, also seeks to "to discourage unconstitutional conduct and to insure integrity in the judicial process by disregarding evidence produced through an impermissible procedure." State v. MacMillan, \_\_\_\_NH \_\_\_\_ (Decided, April 1, 2005.) In short the statute is designed to protect the privacy of individuals and to prohibit a party from benefitting from a violation of another's privacy.

### **RSA 570-A The "Actus Reus"**

In determining the acts which are prohibited by the statute it is necessary to review the definitions contained within the statute itself. See, RSA 570-A:1. As an actual act to be committed the statute requires the "interception" of "telecommunications" or "oral communications" or the disclosure or "use" of the contents of such communications.

Interception. In order to violate the statute one must "intercept" telecommunications or oral communications. The statute defines "interception" as the "aural or other acquisition of, or the recording of, the contents of any telecommunication or oral communication through the use of any electronic, mechanical, or other device."

RSA 570-A:1, III. "Electronic, mechanical, or other device" is defined as

any device or apparatus which can be used to intercept a telecommunication or oral communication other than:

(a) Any telephone or telegraph instrument, equipment, facility or any component thereof:

(1) Furnished to the subscriber or user by a communication carrier 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 in

accordance with applicable provisions of telephone and telegraph company rules and regulations, as approved by the public utilities commission;

(2) Being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties pursuant to this chapter;

(3) Being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

RSA 570-A:1, , IV. The importance of the definition of “interception” was illustrated by the Supreme Court in the case of State v. Telles, 139 NH 344 (1995). In Telles the defendant was charged with aggravated felonious sexual assault against his foster daughter. During a period of time when the foster daughter was visiting with a friend she telephoned the defendant and discussed information which was relevant to their sexual relationship. The friend eavesdropped on that conversation by listening in on another extension phone with in her home. At trial the defendant moved to exclude testimony about the conversations alleging that the friend had violated RSA 570-A:2 and therefore the contents of the conversation should not be permitted to be used at trial. The Court held that listening in on an extension phone did not constitute an “interception” under RSA 570-A:1, III because the definition of an “electronic, mechanical or other device” contained at RSA 570-A:1, IV, exempted any telephone provided to a subscriber in the ordinary course of business. The narrow holding of Telles, is that RSA 570-A:1, IV, (a)(1) creates an absolute exemption for extension phones used in the home by the user or subscriber. See, Telles at p. 347.

However, the reasoning employed by the Telles Court does open the possibility that an absolute domestic relations exception could apply to the state eavesdropping statute. In coming to its ultimate holding the Court stated: "Whether this provision [RSA 570-A:1, IV, (a)(1)] creates an exception for domestic eavesdropping is a question of first impression for this court." Telles at p. 346. The Court went on to review the federal statute which contained similar language and cited with approval to the federal cases: Newcomb v. Ingle, 944 F.2d 1534 (10th Cir.1991) and Anonymous v. Anonymous, 558 F.2d 677, 678-79 (2d Cir.1977). The Telles Court specifically cited that portion of Newcomb wherein the 10th Circuit Court of Appeals found that the federal congress had intended to "to abjure from deciding a very intimate question of familial relations, that of the extent of privacy family members may expect within the home vis-a-vis each other." Telles at p. 347 citing Newcomb at p. 1536. Likewise, in favorably citing Anonymous, the New Hampshire Supreme Court stated:

The Second Circuit affirmed the dismissal of the wife's Title III action, noting that the father's eavesdropping "would clearly not be prohibited if it consisted merely of listening into [sic ] his wife's and daughter's telephone conversations from an extension phone in his apartment. Congress explicitly exempted such activity from coverage by the Act. See 18 U.S.C. § 2510(5)(a)(i)." Anonymous, 558 F.2d at 678 (footnote omitted).

Thus, the reasoning of the Telles decision does leave room to argue that, in New Hampshire, the statute recognizes an absolute domestic relations or spousal exception to the statute. The Supreme Court specifically refused to rule on this question in Fischer v. Hooper, 143 NH 585, 598 (1999). In a domestic relations case the party who was eavesdropping or seeks to use the fruits of such eavesdropping would argue for the broader view of Telles whereas the party resisting the use of such evidence would

argue for the narrow holding of the case.

In an earlier case the New Hampshire Supreme Court held that a police officer executing a search warrant at a suspected drug dealer's home did not "intercept" a communication when he answered a ringing telephone and failed to identify himself as a police officer. See, State v. Lamontagne, 136 NH 575 (1992). In Lamontagne the Court found that the phone calls were not recorded and constituted nothing more than direct communication between the caller and the police officer. The Court found that there was no interception under the circumstances.

**Telecommunications and Oral Communications.** The corpus delicti of a violation of RSA 570-A:2 would be the "telecommunications" or "oral communications" that are intercepted and/or disclosed or used. The statute defines "telecommunications" as "the transfer of any form of information in whole or in part through the facilities of a communications common carrier." RSA 570-A:1, I. "Oral communication" is redundantly defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." RSA 570-A:1,II. It is relevant to note the statutory distinction between "telecommunications" and "oral communications." "Oral communication" requires a finding that the communication was "uttered by a person exhibiting an expectation that such communication is not subject to interception." RSA 570-A:2,IV. In contrast, "telecommunication" does not contain the requirement that the communication has been made under circumstances justifying an expectation of privacy. "Thus, a telephone call, which is a wire communication within this definition, is protected by [the wiretapping statute] regardless of whether the participants actually have any justification

of privacy.” Kratz v. Kratz, 477 F. Supp. 463, 473 (E.D. Pa. 1979). This distinction appears to recognize the commonly held assumption that all telephone calls are secure and are automatically vested with an expectation of privacy. Of course, this assumption is brought into question as telecommunication technology grows into the cellular age.

The New Hampshire Supreme Court addressed at least one aspect of advancing technology in Karch v. Baybank, 147 NH 525 (2002.) In Karch the plaintiff spoke to a friend on a cordless telephone and complained about certain aspects of her employment at the defendant bank. This conversation was overheard by neighbors on a police scanner and recorded. The neighbors subsequently reported the plaintiff's conversation to the defendant bank. The bank disciplined the plaintiff about the phone call. The Plaintiff sued the bank alleging a violation of RSA 570-A because the bank used the contents of the communication to discipline her. The bank alleged that the communication was not protected as a “wire communication” under the version of the statute then in existence because the communication was intercepted between the base of the cordless phone and the handset via the neighbor's scanner. The Court interpreting the 1986 version of the statute made short order of this claim holding:

At the time of the alleged interception of the telephone conversation, RSA 570-A:1, I (1986) defined wire communication as 'any communication made in whole or in part through 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.' We fail to see how the plain language of this definition exempts any part of a cordless telephone conversation from the protections of RSA chapter 570-A. At the very least, a cordless telephone communication includes, in part, 'the use of facilities for the transmission of communications by the aid of wire ... between the point of origin and the point of reception.' *Id.* As such, we find that the communication alleged, 'a wire communication, i.e., by

telephone,' falls within the definition of a wire communication.

Karch v. Baybank, 147 NH 525, 531-532 (2002.) Under the present statute “telecommunications” are protected and defined even more broadly than the term, “wire communication” which was interpreted by the Karch Court. Karch makes it clear that technical detail regarding the stage of transmission of communications will not provide a defense under the state statute.

**Disclosure and/or “use.”** RSA 570-A:2, I, (d) prohibits the willful disclosure or use of the contents of intercepted communications. To date, the New Hampshire Supreme Court has not had occasion to interpret what actions would constitute a disclosure of intercepted communications. However, the court has addressed the “use” element of the statute. In Karch v. Baybank, 147 NH 525 (2002), the defendant, a bank which employed the plaintiff, argued that confronting the plaintiff with the contents of intercepted communications and disciplining the employee as a result of the communication was not the type of “use” envisioned by the statute. The defendants argued that the statute was meant to apply to using the contents of the intercepted conversations in a “court proceeding or for personal gain or similar conduct.” The Karch court found that Baybank’s conduct fell within its own limited definition of the term use. More importantly the court failed to limit the definition of the term “use” to the narrow definition sought by Baybank. . The Court found that there was no such limiting definition within the statute and stated: “. . . we decline to 'redraft [ ] legislation in order to make it conformable to an intention not fairly expressed in it.’” Karch at p. 533 (citations omitted.) Karch suggests that the New Hampshire Supreme Court will broadly interpret the word “use” in the future.

## **RSA 570-A The “*Mens Rea*”**

In order to establish either a criminal violation of the state wiretapping statute or a civil cause of action it must be established that the wiretapper or eavesdropper acted with the requisite *mens rea* or mental state. In Fischer v. Hooper, 143 NH 585 (1999) the Supreme Court held that a wilful violation of the statute required more than acting “knowingly” or being consciously aware, see, RSA 626:2, II, (b), of the act. In *Fischer* an ex-husband, involved in a continuing custody dispute, tape recorded conversations between his ex-wife and their child. No criminal charges were brought, however, an investigation by the attorney general’s office revealed that there had been several surreptitious recordings made of the conversations between mother and child. The ex-wife sued her ex-husband alleging invasion of privacy and violation of RSA 570-A:2. The trial court had instructed the jury that the plaintiff was required only to show that the defendant acted “knowingly.” The Supreme Court reversed and relied upon a number of federal cases which define the term “wilfully.” The Court came to its conclusion after recognizing that the legislature had used two separate mental state requirements when defining the crimes set forth in RSA 570-A:2. The felony level offenses require a “wilful” mental state whereas the misdemeanor offense requires a “knowing” mental state. Although the term wilful is normally equated with the term knowing under New Hampshire law, see, RSA 626:2, IV, the Court found that the use of two separate words demonstrated an intention by the legislature to proscribe two different actions based upon the mental state of the actor. The Court held that a wilful violation meant that:

the defendant must act with an intentional or reckless disregard for the lawfulness of his conduct. In other words,

the defendant has not violated RSA 570-A:2, I, if he has "a 'good faith' belief that [his] conduct was lawful.

Fischer at p. 589 (citations omitted). In essence the violator must have a specific intent to violate the law.

The Court re-affirmed the wilful *mens rea* requirement of Fischer in Karch v. Baybank, 147 NH 525, 532 (2002). In doing so the Karch Court also held that a plaintiff states a claim upon which relief can be granted when she alleges in her writ that the defendant acted wilfully and alleges sufficient facts to support that claim. Karch, p. 532.

### **RSA 570-A Defenses**

New Hampshire's wiretapping statute is fairly complex and the possible defenses to a claim under the statute are limited only by one's imagination. However, two defenses which are repeatedly used are the defense of consent and reliance upon legal authority.

**Consent.** A person may wiretap or eavesdrop if she has obtained the permission of all other parties to the communication. RSA 570-A:2. Such consent may be express or implied. Fischer v. Hooper, 143 NH 585, 597 (1999). In State v. Locke, 144 NH 348, 355 (2000), the Court also held that the person who consents to wiretapping or eavesdropping does not need to be informed of the precise method to be used to monitor the communications. It is sufficient if they consent to monitoring by electronic mechanical or other means. Locke at p. 597. Consent may be implied from the words and/or the conduct of a person under all of the surrounding circumstances. Fischer v. Hooper, 143 NH 585, 598 (1999).

**Legal Authority.** The multitude of various state laws governing wiretapping and eavesdropping as well as the federal statutes have engendered significant confusion about what is, and is not, legal as far as eavesdropping and wiretapping is concerned. Many people believe that they have an absolute right to record, surreptitiously or otherwise, any conversation in which they participate. Indeed many lawyers and public agencies appear to share this belief. In State v. Sheedy, 125 NH 108 (1984), the defendant was charged with violating the wiretapping statute. At trial he attempted to raise the affirmative defense that he had relied upon advice given to him in a letter from the chief engineer of the New Hampshire Public Utilities Commission. From that letter the defendant drew the conclusion that the federal statute, with its one party consent provisions, governed his actions. The defendant sought to raise the affirmative defense set forth at RSA 626:3 which essentially permits reliance upon the statements of law contained within statutes or administrative orders or written interpretations by state agencies. The trial court precluded the defense. The Supreme Court reversed and held that the issue of whether the defendant had relied upon the written interpretation of a state agency was a question of fact and the defendant should have been permitted to raise his defense before the jury. Sheedy at p. 111.

### **Evidentiary and Admissibility Issues**

**Inadmissibility.** The statute itself prohibits the admissibility of recordings made in violation of the statute. RSA 570-A:6 provides:

Whenever any telecommunication or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or

other authority of the state, or a political subdivision thereof, if the disclosure of that information would be in violation of this chapter.

However, the mere fact that the statute was violated may not preclude the contents of the conversation, as opposed to recordings of the conversation, from evidence. In State v. MacMillan, \_\_\_\_ NH \_\_\_\_, 2005 WL 735909, a police officer failed to obtain court approval to monitor and record the contents of an electronic chat room conversation. The actual recording of the chat room conversations were suppressed by the trial judge. However, the trial judge denied the state's motion in limine seeking to admit the officer's testimony about his recollection of the chat room conversations. The state appealed and the Supreme Court reversed the trial judge. The Court essentially held that the officer's recollection of the conversations were not derived from the actual monitoring and therefore his testimony was admissible. See *also*, State v. Stiles, 128 NH 81 (1986.)

**Fifth Amendment Privilege.** In cases involving electronic eavesdropping it is not unusual for a party or witness to seek to exercise the privilege against self incrimination embodied in the Fifth Amendment to the Federal Constitution and Part I Article 15 of the New Hampshire Constitution. When a party or witness invokes the privilege the issue becomes whether the invocation can be used to draw an inference and whether the witness must invoke the privilege in front of the jury or fact finder. In Fischer v. Hooper, 143 NH 585, 598 (1999), the Supreme Court addressed this issue. Relying upon New Hampshire Rule of Evidence 512(b), as it existed at the time, the Court held that it was error for the Court to require the defendant to invoke his Fifth Amendment privilege before the jury and to allow an inference from the invocation.

Fischer at p. 596-597. However, since Fischer, NHRE 512 has been amended by the addition of the following language which was effective on January 1, 2003:

“Subsections (a) to ( c) do not apply in a non-criminal case with respect to the privilege against self-incrimination.” See, NHRE 512 (d). Thus, in a civil or marital proceeding where a party or a witness has violated RSA 570-A:2 and asserted the privilege against self-incrimination the witness may be required to assert the privilege in front of a jury and inferences may be drawn from that assertion.

### **Doctrine of Preemption**

In State v. Kepple, \_\_\_ NH \_\_\_, 866 A.2d 959 (2005), the New Hampshire Supreme Court had the opportunity to determine whether the existence of the less stringent (one party consent) federal statute, 18 USC 2511 *et seq.* , preempts the application of RSA 570-A. The Court specifically held that:

“It is well accepted that Congress' wiretapping statute was not an attempt to occupy the field, but merely an attempt to establish minimum standards.” Whitaker v. Garcetti, 291 F.Supp.2d 1132, 1142 (C.D.Cal.2003). We have recognized that RSA chapter 570-A is more stringent than its federal counterpart, providing more protection for the individual's right to privacy. State v. Ayres, 118 N.H. 90, 91, 383 A.2d 87 (1978) (superseded by statute on other grounds).

The Court went on to find that the state law permissibly provided more privacy protection and therefore was not violative of the federal law nor preempted by the federal statute.

### **Conclusion**

RSA 570-A and its federal counterparts proscribe, for the most part, the surreptitious monitoring and recording of private communications. Although, in some instances such interceptions may, indeed, be legal or admissible, determining when

that may be is a risky venture. The statutes include criminal sanctions and enhanced civil damages. A lawyer faced with these issues should be extremely careful in the advice given and the actions taken to use such communications.

## Appendix

Excerpt from:

UNITED STATES ATTORNEY MANUAL

USAM 9-60.200 et seq.

See,

[http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usam/title9/60mcrm.htm#9-60.200](http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/60mcrm.htm#9-60.200)

## 9-60.200 Criminal Sanctions Against Illegal Electronic Surveillance

Criminal sanctions for illegal electronic surveillance can be found in 18 U.S.C. §§§§ 2510 to 2513, 2701, 3121, 2232(c), 2521, 1367, and 47 U.S.C. §§§§ 605, 553, 502. Supervisory responsibility for these offenses rests with the Computer Crime and Intellectual Property Section of the Criminal Division.

See the following sections of the Criminal Resource Manual for an overview of the criminal sanctions against illegal electronic surveillance, including related definitions and terms

Criminal Sanctions for Illegal Electronic Surveillance	Criminal Resource Manual at 1040
Investigative Jurisdiction and Supervisory Responsibility	Criminal Resource Manual at 1041
Legislative History	Criminal Resource Manual at 1042
Definition -- "Wire Communication"	Criminal Resource Manual at 1043
Definitions -- "Oral Communication"	Criminal Resource Manual at 1044
Definition -- "Electronic Communication"	Criminal Resource Manual at 1045
Definition -- "Intercept"	Criminal Resource Manual at 1046
Definition: "Electronic, Mechanical, or Other Device"	Criminal Resource Manual at 1047
Definition -- "Person"	Criminal Resource Manual at 1048
Definition -- "Contents"	Criminal Resource Manual at 1049
Scope of 18 U.S.C §§ 2511 Prohibitions	Criminal Resource Manual at 1050
"Intentional" State of Mind	Criminal Resource Manual at 1051
Elements of Section 2511 Offenses	Criminal Resource Manual at 1052
Exceptions to the Prohibitions Against Intercepting Communications -- Interceptions by Providers of Wire or Electronic Communications Services	Criminal Resource Manual at 1053

Exceptions to the Prohibitions-- Consensual Law Enforcement Interceptions	Criminal Resource Manual at 1054
Exceptions to the Prohibitions -- Other Consensual Interceptions	Criminal Resource Manual at 1055
Exceptions for the Interception of Certain Communications	Criminal Resource Manual at 1056
Other Exceptions	Criminal Resource Manual at 1057
Penalties	Criminal Resource Manual at 1058
Use of the Contents of Illegally Intercepted Communications Against the Interceptor	Criminal Resource Manual at 1059
Scope of 18 U.S.C §§ 2512 Prohibitions	Criminal Resource Manual at 1060
Unlawful Access to Stored Communications -- 18 U.S.C. §§ 2701	Criminal Resource Manual at 1061
Unauthorized Installation or Use of Pen Registers and Trap and Trace Devices -- 18 U.S.C. §§ 3121	Criminal Resource Manual at 1062
Providing Notice of Electronic Surveillance -- 18 U.S.C. §§ 2232(c)	Criminal Resource Manual at 1063
Injunctions Against Illegal Interception -- 18 U.S.C. §§ 2521	Criminal Resource Manual at 1064
Interference With the Operation of a Satellite -- 18 U.S.C. §§ 1367	Criminal Resource Manual at 1065
Interception of Radio Communications -- 47 U.S.C. §§ 605	Criminal Resource Manual at 1066
Unauthorized Reception of Cable Service -- 47 U.S.C. §§ 553	Criminal Resource Manual at 1067
Violation of FCC Regulations -- 47 U.S.C. §§ 502	Criminal Resource Manual at 1068

## 9-60.202 Illegal Electronic Eavesdropping -- Prosecution Policy

The criminal prohibitions against illegal electronic eavesdropping contained in Title III are part of the same act which permits federal law enforcement officers to engage in court-authorized electronic surveillance. Congress viewed the criminal sanctions and the court authorization provisions as two sides of the same coin. The retention of the government's authorization to engage in court-authorized electronic surveillance may depend on its vigorous enforcement of the sanctions against illegal electronic eavesdropping. Accordingly, it is the Department's policy to vigorously enforce these criminal prohibitions.

The Department's overall prosecutive policy under 18 U.S.C. §§ 2511 is to focus primarily on persons who engage or procure illegal electronic surveillance as part of the practice of their profession or as incident to their business activities. Less emphasis should be placed on the prosecution of persons who, in the course of transitory situations, intercept communications on their own without the assistance of a professional wiretapper or eavesdropper. This does not mean that such persons are never to be prosecuted, but simply that this type of prosecution is not a major thrust of the Department's enforcement program.

Most illegal interceptions fall into one of five categories: (1) domestic relations, (2) industrial espionage, (3) political espionage, (4) law enforcement, and (5) intra-business. The largest number of interceptions, more than 75 percent, are in the domestic relations category. It is the Department's policy to vigorously investigate and prosecute illegal interceptions of communications which fall within the industrial and political espionage, law enforcement, and intra-business categories. Generally such violations will have interstate ramifications which will make federal prosecution preferable to state prosecution. Nevertheless, in cases where the federal interest is slight, it may be appropriate to defer to state prosecution.

Illegal interceptions arising from domestic relations disputes generally present less of a federal interest and, therefore, local prosecution is more appropriate. However, this does not mean that federal prosecutors should abdicate responsibility for prosecuting such interceptions. Indeed, in view of the preponderance of this kind of interception, no enforcement program can be effective without the initiation of some prosecutions for deterrence purposes. United States Attorneys should develop effective liaison with local prosecutors in order to convince them to shoulder their share of the burden.

Within the category of domestic relations violations, primary attention should be given to those instances in which a professional is involved, such as a private detective, attorney, moonlighting telephone company employee, and supplier of electronic surveillance devices. United States Attorneys should feel free to pursue these cases or refer them to local prosecutors; however, no professional should escape prosecution when a prosecutable case exists.

Domestic relations violations which do not involve a professional interceptor are the lowest priority cases for federal prosecution. Although local prosecution is normally

preferable, when local prosecutors are unwilling to pursue the case, resort to federal prosecution may be appropriate. Nevertheless, violations of this type will sometimes prove to be of insufficient magnitude to warrant either federal or state prosecution. In such cases, other measures may prove sufficient, for example, a civil suit for damages (18 U.S.C. §§ 2520), suppression of evidence (18 U.S.C. §§ 2515), or forfeiture of the wiretapping or eavesdropping paraphernalia (18 U.S.C. §§ 2513).

Disturbed persons often suspect that they are the victims of illegal interceptions. Consequently, a complaint which is based solely on suspicious noises heard on the telephone normally does not merit further investigation if the initial line check fails to produce independent evidence of a tap.

#### 9-60.203 State Laws

Title III does not preempt the authority of the states to legislate concerning the interception of communications. The protection of privacy is as much a matter for local concern as protection of persons and property. Accordingly, the efforts of federal law enforcement personnel should supplement, not supplant, local action.

United States Attorneys should review the applicable statutes in their states. When there is no statute or when the existing statutes are inadequate, United States Attorneys should work through their federal-state law enforcement committees to obtain the enactment of appropriate legislation. When suitable state legislation exists but is not sufficiently used by local prosecutors, United States Attorneys should make efforts to stimulate local enforcement.

#### 9-60.262 Prosecutive Policy -- 18 U.S.C. §§ 2512

Flagrant violators of 18 U.S.C. §§ 2512 should be prosecuted vigorously, especially violators who possess such devices in order to engage in electronic surveillance as a business.

Less culpable first offenders and those who violate the statute because of ignorance of the law may be appropriate subjects for more lenient disposition. In some cases a warning may be sufficient. Nevertheless, in all cases except, perhaps, for minor advertising violations, the United States Attorney's Office should require that the prohibited device either be surrendered voluntarily to the FBI or forfeited pursuant to 18 U.S.C. §§ 2513.