

## COMMENTS

# E-MAIL AND VOICE MAIL: EMPLOYEE PRIVACY AND THE FEDERAL WIRETAP STATUTE

THOMAS R. GREENBERG\*

## TABLE OF CONTENTS

Introduction .....	220
I. Current Statutory Framework .....	225
A. Title III .....	225
1. Limitations of the 1968 version of Title III ....	227
2. When is an interception not an interception? ..	228
a. <i>United States v. Christman</i> .....	228
b. Other court decisions .....	230
B. The Electronic Communications Privacy Act of 1986 .....	231
1. Expanded coverage of the ECPA .....	232
2. Retention of pre-ECPA statutory exceptions ...	234
a. "Extension telephone" and "ordinary course of business" exceptions .....	235
b. System provider exception .....	236
c. Exceptions under the stored communications provisions .....	238
II. Statutory Exceptions for Private Employers .....	238
A. "Legitimate Business Purpose" Cases .....	239
B. "Subject of the Call" Cases .....	241

---

\* J.D. Candidate, May 1995, The American University, Washington College of Law. The number of people contributing to this Article are too numerous to mention. My wife, Elaine, however, deserves special mention for her limitless indulgence, not only with the many drafts of this Article, but throughout my law school career.

III. The Statutory Framework Meets the Modern Technologies . . . . .	246
A. Comparing the Cases to E-Mail and Voice Mail . . .	246
B. Irrationality of Title III . . . . .	247
IV. Recommendations . . . . .	249
A. Employers . . . . .	249
B. Statutory Reform . . . . .	250
Conclusion . . . . .	252

## INTRODUCTION

Twenty-seven years ago, the U.S. Supreme Court ruled in *Katz v. United States*<sup>1</sup> that the Fourth Amendment<sup>2</sup> to the U.S. Constitution "protects people not places."<sup>3</sup> Despite the Supreme Court's endorsement of individual privacy rights in general, the Court in *Katz* did not extend its endorsement to the employees of private companies. The Fourth Amendment does protect against "unreasonable" searches and seizures,<sup>4</sup> and the Supreme Court has held that the prohibition against such unwarranted intrusions extends to federal, state, and local government employees in cases of searches made by their employers.<sup>5</sup> Private sector employees, however, do not benefit from this Fourth Amendment protection where a search is conducted by their employer in a non-law enforcement capacity.<sup>6</sup>

---

1. 389 U.S. 347 (1967).

2. U.S. CONST. amend. IV. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

3. *Katz v. United States*, 389 U.S. 347, 351 (1967). *Katz* overruled *Olmstead v. United States*, 277 U.S. 438 (1928), which concluded that wiretapping did not violate the Fourth Amendment because no actual physical intrusion takes place. *Olmstead*, 277 U.S. at 466. *Katz* held that the Fourth Amendment protects individuals against unauthorized interception of their telephone communications by the Government. *Katz*, 389 U.S. at 350.

4. See *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (stating that although Fourth Amendment protects against unreasonable searches and seizures, determining whether search is reasonable depends in part on existence of reasonable expectation of privacy).

5. *Id.* at 724-25. In *O'Connor*, the Court considered the applicability of Fourth Amendment privacy rights to non-court-ordered searches of public employee's offices. *Id.* at 711-12. In that case, a state-run hospital in California, having been made aware of allegations of wrongdoing by an employee, searched the employee's office and confiscated personal items. *Id.* at 713. The Court concluded that the employee had a reasonable expectation of privacy within the confines of his office. *Id.* at 718. Therefore, government employers must first have reasonable grounds for making warrantless searches. *Id.* at 724-25.

6. See Alfred G. Feliu & Wayne N. Outten, *Privacy in the Employment Relationship*, in 2 PRIVACY LAW AND PRACTICE ¶ 9.02[3][d] (George B. Trubow ed., 1991) (noting that employees of private companies do not enjoy Fourth Amendment constitutional protections from employer searchers, as do their publicly employed counterparts).

The lack of constitutional protection for private sector employees has been made all the more critical by technological advances in the workplace. In particular, growing reliance by businesses on E-mail<sup>7</sup> and voice mail<sup>8</sup> communications systems has created many new opportunities for private sector employers to monitor the performance and conduct of their employees without the employees knowing.<sup>9</sup> The risks to the privacy of workplace communications were recently evidenced by a survey of 301 employers conducted by *Macworld* magazine.<sup>10</sup> In this survey, *Macworld* sought information from employers in a broad spectrum of industries regarding the extent to which the employers monitor employee computer, E-mail, and voice mail systems.<sup>11</sup> The results showed that twenty-two percent of the respondents had "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communica-

---

7. E-mail is the common term used for electronic mail, and encompasses a number of differing technologies. See HOUSE COMM. ON THE JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, H.R. REP. NO. 647, 99th Cong., 2d Sess. 22 [hereinafter H.R. REP. NO. 647]. Congress described E-mail as a service that allows two parties to "transmit a digital message" between two computer terminals through a service provider, where it is maintained in electronic storage until accessed by the recipient. *Id.* at 63. In the context of data communications, the term "digital" describes the binary output of a computer. DANIEL ABELOW & EDWIN J. HILPERT, COMMUNICATIONS IN THE MODERN CORPORATE ENVIRONMENT 225 (1986). A digital signal can only be one of two discrete units (off/on). *Id.*; see also Russell S. Burnside, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies*, 13 RUTGERS COMPUTER & TECH. L.J. 451, 483 n.213 (1987) (describing E-mail as service that allows two parties to send messages via third-party routing service).

As of 1992, estimates showed that 20 million Americans were a part of an E-mail service. *Electronic Mail Raises Issues About Privacy, Experts Say*, Daily Lab. Rep. (BNA) No. 222, at A-7, A-8 (Nov. 17, 1992). Projections indicate that E-mail usage will be double the 1992 estimate by the turn of the century, with some 60 billion messages being transmitted per year. Scott Dean, *E-Mail Forces Companies to Grapple with Privacy Issues*, CORP. LEGAL TIMES, Sept. 1993, at 11.

8. During congressional consideration of the Electronic Communications Privacy Act of 1986, Congress noted that "voice mail" was similar to E-mail, and operated in a similar manner. H.R. REP. NO. 647, *supra* note 7, at 63. Voice mail, however, differs from E-mail in that the messages take "the form of the sender's voice." *Id.*

Voice mail systems generally "consist of some type of computer, an analog-to-digital voice processing subsystem, disk storage, and software to provide the mailbox and answering machine environment." STEPHEN A. CASWELL, E-MAIL 191 (1988). The human voice in this context is digitized directly by the computer and stored as a digital pattern. JOSEPH ST. JOHN BATE, MANAGEMENT GUIDE TO OFFICE AUTOMATION 163 (1987). The computer "listens to" and duplicates, in digital form, the entire voice message of the sender. *Id.* On the receiving end, the digital message is converted back to analog form and emerges as a voice over the telephone. *Id.* The term analog, as used in data communications, describes the wave or signal (such as the human voice), whose value changes continuously. ABELOW & HILPERT, *supra* note 7, at 223. For such waves to be transmitted over a telephone line, a digital or pulse output must be converted to an analog signal. *Id.*

9. See Charles Piller, *Bosses With X-Ray Eyes*, MACWORLD, July 1993, at 118, 123 (chart) (indicating that 66.2% of employers responding to survey who engage in monitoring did not inform employees that monitoring was taking place).

10. *Id.* at 123.

11. *Id.* at 120.

tions."<sup>12</sup> Of that twenty-two percent of employers, slightly more than sixty-six percent of them confirmed that they conducted employee monitoring without the employees' knowledge or consent.<sup>13</sup>

Given the apparent scope of employer monitoring and the rate at which new technologies are being introduced into the workplace, what, if any, right of confidentiality should employees of private companies expect in their communications? A partial answer to this question may be found in the remedies provided by Title III of the Omnibus Crime Control and Safe Streets Act of 1968<sup>14</sup> (Title III), and the Electronic Communications Privacy Act of 1986<sup>15</sup> (ECPA), which substantially amended Title III.<sup>16</sup> These provisions, commonly

12. *Id.* The MACWORLD investigation further found that in companies with 1000 or more employees, the number of employers indicating that they had monitored employee communications rose to 30%. *Id.* Applying this percentage to the American workforce, Charles Piller, the article's author, estimates that the extent of employer workplace monitoring encompasses approximately 20 million workers based on computer systems alone, i.e., excluding employer monitoring of basic telephone systems. *Id.* The *Macworld* survey received responses indicating that 41.5% of the companies accessed employee E-mail systems, 15.4% listened to employee voice mail messages, 73.8% had perused employee's electronic work files, and 27.7% had accessed employee network messages. *Id.* at 123 (chart). The apparent willingness of employers to eavesdrop on employee communications, as evidenced by the *Macworld* study, is in sharp contrast to the belief by employees that their communications are private and should not be monitored by employers even if the capability to monitor exists. See Caroline M. Cooney, *Who's Watching the Workplace? The Electronic Monitoring Debate Spreads to Capitol Hill*, SECURITY MGMT., Nov. 1991, at 26, 29 (citing August 1991 reader survey conducted by *Nation's Business*, in which 64% of respondents indicated that employers should be required to notify employees in advance of employer monitoring and 25% believed that employers should notify employees when monitoring is actually occurring).

13. Piller, *supra* note 9, at 118, 123 (chart).

14. Pub. L. No. 90-351, §§ 801-804, 82 Stat. 197, 211-25 (codified as amended at 18 U.S.C. §§ 2510-2521 (1988 & Supp. V 1993)).

15. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988 & Supp. V 1993)).

16. Title III and the ECPA are by no means the only source of redress for an employee aggrieved by employer workplace monitoring. In addition to other federal enactments protecting privacy, such as the Communications Act of 1934, 47 U.S.C. § 605 (1988), and FCC regulations, 47 C.F.R. § 2.701 (1993), and common law tort claims for invasion of privacy, the following state legislatures have created their own private rights of action for illegal wiretapping, which substantially parallel federal law. Most of these states award actual or statutory damages of \$100 per day of violation or \$1000, whichever is greater, in addition to reasonable attorney's fees and costs. See CAL. PENAL CODE ANN. § 629.36 (West Supp. 1994) (establishing civil remedies for any person whose wire or oral communication is intercepted, including actual damages, "but not less than liquidated damages" of \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, reasonable attorney's fees, and other costs of litigation); DEL. CODE ANN. tit. 11, § 1336(w) (1987) (establishing civil remedy for any person whose wire or oral communications are intercepted and allowing for recovery of either actual damages or statutory damages of \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, attorney's fees, and litigation costs); D.C. CODE ANN. § 23-554(a) (1981) (providing civil remedies for any person whose wire or oral communications are intercepted, including actual damages or greater of liquidated damages of \$100 per day for each day of violation or \$1000, punitive damages, reasonable attorney's fees, and costs); FLA. STAT. ANN. ch. 934.10 (1993) (establishing private right of action for any person whose wire or oral communication is intercepted and allowing for recovery of actual damages or statutory damages of either \$100 per day for each day violation continued, or \$1000,

whichever is greater, punitive damages, reasonable attorney's fees, and costs); HAW. REV. STAT. § 803-48(A)-(C) (1985 & Supp. 1992) (providing civil remedy for any person whose wire, oral, or electronic communications are accessed or intercepted and allowing for recovery of actual damages or greater of liquidated damages of \$100 per day for each day of violation or \$10,000, punitive damages, reasonable attorney's fees, and court costs, or equitable or declaratory relief where appropriate); IDAHO CODE § 18-6709 (1987) (creating private right of action for any person whose wire or oral communications are intercepted and allowing for recovery of either actual damages or statutory damages of \$100 per day for each day of violation or \$1000, whichever is greater, punitive damages, reasonable attorney's fees, and litigation costs); ILL. ANN. STAT. ch. 720, para. 5/14-6(1) (Smith-Hurd 1993) (providing for civil remedies where eavesdropping on conversation has occurred, and allowing for injunction against further eavesdropping, and actual and punitive damages); IND. CODE ANN. § 35-33.5-5-4(a) (1993) (establishing private right of action for any person whose communications are intercepted, and providing for recovery of either actual damages, but not less than liquidated damages of \$100 per day for each day of violation or \$1000, whichever is greater, punitive damages, reasonable attorney's fees, and court costs); IOWA CODE ANN. § 808B.8.1 (extended to July 1, 1999) (West 1994) (allowing any party whose wire or oral communications are intercepted to recover greater of actual damages or statutory damages of not less than \$100 per day for each day of violation or \$1000, punitive damages, attorney's fees, and costs); KAN. STAT. ANN. § 22-2518(1) (1988) (establishing private right of action for any person whose wire, oral, or electronic communications are intercepted, and allowing for recovery of actual damages or statutory damages of either \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, reasonable attorney's fees, and costs); ME. REV. STAT. ANN. tit. 15, § 711 (West 1980 & Supp. 1993) (creating civil remedy for any person whose conversation is intercepted in violation of this section, and providing for recovery of actual damages, but not less than liquidated damages of \$100 per day for each day of violation, attorney's fees, and costs); MD. CODE ANN., CTS. & JUD. PROC. § 10-410(a) (1993) (providing civil remedy for any person whose wire, oral, or electronic communications are intercepted and allowing recovery of either actual damages, or greater of statutory damages of \$100 per day for each day violation continued, or \$1000, punitive damages, attorney's fees, and costs); MASS. GEN. LAWS ANN. ch. 272, § 99Q (West 1990) (establishing civil remedy for any person whose wire or oral communications are intercepted, and providing for recovery of either actual damages or statutory damages of \$100 per day for each day violation continued, or \$1000, whichever is greater, punitive damages, attorney's fees, and costs); MICH. COMP. LAWS ANN. § 750.539h (West 1991) (allowing any party on whom eavesdropping is practiced to receive an injunction, and actual and punitive damages); MINN. STAT. ANN. § 626A.13(1)-(3) (West 1983 & Supp. 1994) (providing civil remedy for any person whose wire, electronic, or oral communication is intercepted, and allowing for temporary or other equitable or declaratory relief, treble damages or statutory damages of \$100 per day for each day of violation or \$10,000, whichever is greater, attorney's fees, and litigation costs); MISS. CODE ANN. § 41-29-529(1) (1993) (establishing civil remedy for any person whose wire or oral communications are intercepted and allowing for recovery of actual damages or statutory damages of \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, attorney's fees, and costs); NEB. REV. STAT. § 86-707.02 (Supp. 1992) (creating private right of action for any person whose wire, oral, or electronic communications are intercepted, and providing for preliminary or equitable or declaratory relief, actual damages or greater of statutory damages of \$100 per day for each day of violation or \$10,000, and attorney's fees); N.H. REV. STAT. ANN. § 570-A:11 (1986) (providing civil action to any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); N.J. STAT. ANN. § 2A:156A-24(a)-(c) (West 1985 & Supp. 1994) (extended to July 1, 1999) (establishing private right of action for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); N.M. STAT. ANN. § 30-12-11(A) (Michie 1984) (establishing private right of action for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); OHIO REV. CODE ANN. § 2933.65(A) (Baldwin 1992) (establishing private right of action for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or \$200 per day for

referred to as the Wiretap statute,<sup>17</sup> have been judicially interpreted to offer a limited degree of privacy protection for the telephone communications of private-company employees.<sup>18</sup> Whether such protection extends to E-mail and voice mail communications is presently unclear, although some commentators have suggested that Title III and the ECPA do not encompass these technologies with respect to private employers.<sup>19</sup> This Comment argues that the intent

---

each day violation continued up to \$2000, punitive damages, attorney's fees, and costs); OR. REV. STAT. § 133.739(1) (1993) (providing civil cause of action to any person whose wire, oral, or electronic communications are intercepted and allowing recovery of actual damages, but not less than \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, and attorney's fees at trial and on appeal); CRIMES & OFFENSES PA. CONS. STAT. ANN. § 5725(a) (1983 & Supp. 1992) (creating private right of action for any person whose wire, oral, or electronic communications are intercepted and allowing for recovery of actual damages or greater of statutory damages of \$100 per day for each day of violation or \$1000, punitive damages, attorney's fees, and costs); R.I. GEN. LAWS § 12-5.1-13 (1981) (establishing civil remedy for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and litigation costs); UTAH CODE ANN. § 77-23a-11(1)-(3) (1990) (providing private right of action for any person whose wire, oral, or electronic communications are intercepted and allowing for preliminary or other equitable or declaratory relief as appropriate or statutory damages of \$100 per day for each day of violation or \$10,000, whichever is greater, punitive damages and, attorney's fees, and costs); VA. CODE ANN. § 19.2-69 (Michie 1990) (establishing civil cause of action for any person whose wire, oral, or electronic communications are intercepted and allowing for recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); WASH. REV. CODE § 9.73.060 (1992) (providing private right of action for any person whose privacy is violated within meaning of this chapter and allowing recovery of actual damages, including mental pain and suffering, or statutory damages of \$100 per day for each day of violation up to \$1000, attorneys fees, and costs); W. VA. CODE ANN. § 62-1D-12(a) (1992) (establishing civil remedy for any person whose wire, oral, or electronic communications are intercepted and allowing for recovery of actual damages, but not less than \$100 per day for each day violation continued, punitive damages, attorney's fees, and costs); WIS. STAT. ANN. § 968.31(2m) (West Supp. 1993) (providing civil remedy for any person whose wire, oral, or electronic communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); WYO. STAT. § 7-3-609(a) (1987 & Supp. 1993) (creating private right of action for any person whose wire, oral, or electronic communications are intercepted and allowing recovery of actual damages, but not less than \$1000 per day for each day violation continued, punitive damages, attorney's fees, and costs).

Further, many states recognize both common law and statutory rights to privacy, which can be used as the basis for civil damages against invasions of privacy. See *Privacy for Consumers and Workers Act: Hearing on S.984 Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor & Human Resources*, 101st Cong., 1st Sess. 23-24 (1993) (Statement of Lewis L. Maltby, Director, ACLU National Task Force on Civil Liberties in the Workplace) (noting that almost all states have common law right to privacy, but recognizing limitation of common law in employment context). This Comment, however, focuses only on the private rights of action created under Title III and the ECPA.

17. See S. REP. NO. 541, 99th Cong., 2d Sess. 3 (1986), reprinted in 1986 U.S.C.A.N. 3555, 3556-57.

18. See *infra* Part II (discussing cases applying Federal Wiretap Statute as source of protection for private telephone conversations made at workplace).

19. See, e.g., Ruel T. Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 39 (1987) (stating that under stored communications provisions of ECPA, employer will not be liable for accessing E-mail or voice mail communications of employees, even where third parties would be liable for similar conduct); Holly Metz, *They've Got Their Eyes on You*, STUDENT LAW.,

of Title III and the ECPA, based on the extensive legislative histories supporting both enactments, was to enhance privacy protection, irrespective of technological advancement, but that current judicial application of Title III and the ECPA falls short of this intent.

Part I of this Comment reviews the language of Title III and the ECPA, and attempts to decipher Congress' intent with respect to employer monitoring. Part II examines the judicial application of Title III and the ECPA in the workplace monitoring context. Part III uses the existing case law to analogize the applicability of these provisions to employee privacy rights with respect to E-mail and voice mail systems, and attempts to reconcile the inconsistent court holdings arising from differing interpretations of the statutes.<sup>20</sup> Finally, Part IV of this Comment recommends that Congress modify Title III and the ECPA to affirmatively bring emerging office technologies within the purview of these statutes.

## I. CURRENT STATUTORY FRAMEWORK

### A. *Title III*

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 was the first congressional response to the Supreme Court's holding in *Katz*.<sup>21</sup> Congress intended Title III to comprehensively

---

Feb. 1994, at 22, 23 (citing Lewis Maltby, attorney for ACLU, who states that employees in private sector have no legal recourse under existing legislation); Julia T. Baumhart, Comment, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923, 926 (1992) (arguing that lack of discussion about issue in legislative history of ECPA indicates Congress did not intend statute to prevent employers from accessing employee E-mail).

20. The difficulty federal courts have had in determining the applicability of Title III in the context of employer workplace monitoring was well expressed by Judge Charles C. Goldberg of the Fifth Circuit:

We might wish we had planted a powerful electronic bug in a Congressional antechamber to garner every clue concerning Title III, for we are once again faced with the troublesome task of an interstitial interpretation of an amorphous Congressional enactment. Even a clear bright beam of statutory language can be obscured by the mirror of Congressional intent. Here, we must divine the will of Congress when all recorded signs point to less than full reflection. But, alas, we lack any sophisticated sensor of Congressional whispers, and are remitted to our more primitive tools. With them, we can only hope to measure Congress' general clime. So we engage our wind vane and barometer and seek to measure the direction of the Congressional vapors and the pressures fomenting them. Our search for lightening bolts of comprehension traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal.

*Briggs v. American Air Filter Co.*, 630 F.2d 414, 415 (5th Cir. 1980).

21. See OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 18 (1985) [hereinafter *ELECTRONIC SURVEILLANCE*] (noting that Title III was first major congressional action concerning surveillance and was drafted to conform with *Katz*).

regulate the use of wiretaps and hidden microphones<sup>22</sup> on all communications transmitted via common carrier.<sup>23</sup> Although Congress intended Title III to regulate primarily Government use of wiretaps and other surveillance media,<sup>24</sup> the statute applies to private individuals and businesses as well.<sup>25</sup> Specifically, § 2511 of Title III prohibited the actual or attempted willful interception of any "wire or oral communication";<sup>26</sup> the actual or attempted willful use of

22. See *id.* at 3.

23. Section 2510(10) of Title III defines a "communication common carrier" by cross-reference to the ambiguous definition of that term contained in the Communications Act of 1934: "any person engaged as a common carrier for hire, in interstate or foreign communication by wire." 47 U.S.C. § 153(h) (1988). Federal Communications Commission regulations are equally vague, defining a communications common carrier as "[a]ny person engaged in rendering communication service for hire to the public." 47 C.F.R. § 21.2 (1993). Fortunately, the courts have clarified these circuitous definitions. In *National Ass'n of Regulatory Utility Commissioners v. FCC*, the court summarized the criteria a company must meet in order to be considered a communications common carrier. *National Ass'n of Regulatory Util. Comm'rs v. FCC*, 533 F.2d 601, 608 (D.C. Cir. 1976). The company must have a quasi-public character and must provide similar service to all potential and willing users, even if the service is specialized or the number of potential users is limited. *Id.*; see also *National Ass'n of Regulatory Util. Comm'rs v. FCC*, 525 F.2d 630, 641 (D.C. Cir.) (stating that carrier falls within definition of common carrier if it does not "make only individualized decisions, in particular cases, whether and on what terms to deal"), *cert. denied*, 425 U.S. 992 (1976). This "public" criterion is the key distinction between public common carriers and private companies, the latter providing service to particular customers of the company's own choosing. *National Ass'n of Regulatory Util. Comm'rs*, 525 F.2d at 642.

24. See S. REP. NO. 1097, 90th Cong., 2d Sess. 70-76 (1968), *reprinted* in 1968 U.S.C.A.N. 2112, 2157-63 (explaining that Wiretap statute's main purpose is to regulate use of wiretapping and electronic surveillance by law enforcement officials in combatting organized crime); Martha W. Barnett & Scott D. Makar, "In the Ordinary Course of Business": *The Legal Limits of Workplace Wiretapping*, 10 HASTINGS COMM. & ENT. L.J. 715, 718 (1988) (stating that primary purpose of federal wiretap statute is to regulate law enforcement, but noting that statute also applies to individuals and corporations).

25. Barnett & Makar, *supra* note 24, at 718. The Commerce Clause of the Constitution provides authority for federal control of wiretapping. See *Weiss v. United States*, 308 U.S. 321, 327 (1939). The Supreme Court has upheld federal legislation prohibiting wiretapping of interstate or intrastate telephone conversations by federal and state law enforcement officers. See *Weiss*, 308 U.S. at 327 (suppressing evidence of insurance fraud gained through interception of intrastate telephone communications without authorization); *Nardone v. United States*, 302 U.S. 379, 382 (1937) (holding that evidence gained by tapping interstate phone conversations was not admissible under statute prohibiting interception of such communication unless authorized by statute). Legislation prohibiting wiretapping by private persons may also be adopted and enforced by the Federal Government under the Commerce Clause. See *United States v. Gris*, 247 F.2d 860, 863 (2d Cir. 1957) (rejecting argument of defendant convicted of illegal private wiretapping that only interstate, not intrastate, communications are protected).

26. Pub. L. No. 90-351, § 802, 82 Stat. 197, 213 (1968) (codified as amended at 18 U.S.C. § 2511(1)(a) (1988)). Title III defined a "wire communication" as "any communication made in whole or in part through the use of [common carrier] facilities for the [interstate or foreign] transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." *Id.* at 212 (codified as amended at 18 U.S.C. § 2510(1)). An "oral communication" was defined as "any oral communication uttered by a person exhibiting an expectation [of privacy]." *Id.* (codified as amended at 18 U.S.C. § 2510(2)). The term "interception" is defined as an "aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." *Id.* (codified as amended at 18 U.S.C. § 2510(4)).



"electronic, mechanical or other device to intercept any oral communication";<sup>27</sup> and the actual or attempted willful disclosure or use of "the contents of any wire or oral communication."<sup>28</sup> Section 2520 of Title III established a private right of action for these enumerated violations of § 2511.<sup>29</sup>

### 1. *Limitations of the 1968 version of Title III*

Congress enacted Title III at a time when the primary means for intercepting communications was "limited . . . to simple telephone taps and concealed microphones,"<sup>30</sup> and the two primary modes of communication were either "telephone conversations"<sup>31</sup> or "face-to-face oral communications."<sup>32</sup> While Title III reflected the prevalent technologies of the era, it failed to account for future developments.<sup>33</sup> Title III expressly protected against only the unauthorized aural interception of a communication.<sup>34</sup> Thus, there was no Title III protection against the interception of "text, digital or machine communication"<sup>35</sup> because in these sources of communication, there are no audible sounds to intercept. In addition, for wire communications, the statute protected only those communications traversing the facilities of a common carrier, while for oral communications, only

---

27. *Id.* at 215 (codified as amended at 18 U.S.C. § 2511(1)(b)).

28. *Id.* (codified as amended at 18 U.S.C. § 2511(1)(c)-(d)).

29. *See id.* at 223 (codified as amended at 18 U.S.C. § 2520) (providing that any person may bring civil cause of action against any person who intercepts, discloses, or uses any wire or oral communication). Under § 2520, damages are the greater of the sum of actual damages or statutory damages of \$100 per day of violations or \$10,000, whichever is greater. Attorney's fees and costs also may be awarded to a successful plaintiff. 18 U.S.C. § 2520(c)(2).

30. ELECTRONIC SURVEILLANCE, *supra* note 21, at 3.

31. H.R. REP. NO. 647, *supra* note 7, at 17. The House report on the ECPA noted that even though Title III was less than 20 years old, it reflected a "different technological and regulatory era" where "[c]ommunications were almost exclusively in the form of transmission of the human voice over common carrier networks . . . [and] the contents of a traditional telephone call disappeared once the words [were] transmitted." *Id.*

32. H.R. REP. NO. 647, *supra* note 7, at 17.

33. *See* H.R. REP. NO. 647, *supra* note 7, at 17 (stating that Congress "did not attempt to address the interception of text, digital or machine communication").

34. 18 U.S.C. § 2510(4) (1988) (providing that "interception," by definition, can only be accomplished through "aural acquisition" of contents of "any wire or oral communication"). "Aural" involves acquisition through the sense of hearing. There is no statutory definition of "aural." As noted by the U.S. Court of Appeals for the Fourth Circuit, lacking a statutory definition, the meaning ascribed should be the one commonly accepted. *United States v. Seidlitz*, 589 F.2d 152, 157 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979); *see also* *United States v. Bynum*, 360 F. Supp. 400, 408 (S.D.N.Y.) (stating that under § 2510(4), term "intercept" unambiguously equates "with listening to, monitoring, or hearing"), *aff'd*, 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974); *Smith v. Wunker*, 356 F. Supp. 44, 46 (S.D. Ohio 1972) (noting that literal understanding of "aural acquisition" means to "come into possession through the sense of hearing").

35. H.R. REP. NO. 647, *supra* note 7, at 17 (recognizing that these forms of communication were not as common as telephone communication or face-to-face oral communication).

conversations made under conditions demonstrating a reasonable expectation of privacy were protected.<sup>36</sup>

2. *When is an interception not an interception?*

The 1968 version of Title III provided that an oral or wire communication was intercepted only if aurally acquired through the use of "any electronic, mechanical, or other device."<sup>37</sup> Efforts by federal courts to construe the meaning of this language have led to disparate results.<sup>38</sup> One of the first cases to test Title III in a private employer context was *United States v. Christman*.<sup>39</sup> Although *Christman* involved a criminal prosecution and not a suit for civil damages,<sup>40</sup> the district court still addressed whether Title III's protection applied to communications transmitted via a private phone system.<sup>41</sup>

a. *United States v. Christman*

In the 1974 case *United States v. Christman*, the defendant, a security manager for a department store, was charged with illegally intercepting and recording an employee's telephone calls by using an extension telephone in violation of 18 U.S.C. § 2511(1)(a), which prohibited, *inter alia*, the interception of a wire communication.<sup>42</sup> The defendant's employer operated a "closed dial" telephone system, which allowed employees to place calls within the store, and to other stores in the same chain.<sup>43</sup> The "closed dial" system could be used to place outside calls, but such calls required the assistance of a switchboard operator, and, in any event, were strictly limited to "special circumstances."<sup>44</sup> In response to allegations that the store's telephone system was being used for improper purposes, and in some instances for illegal conduct, the defendant installed an extension

---

36. H.R. REP. No. 647, *supra* note 7, at 17 (noting that passage of Title III was Congress' response to unregulated ability of Government to eavesdrop, but that Title III still provides for permissible government interception of communications).

37. 18 U.S.C. § 2510(4).

38. Compare *United States v. Christman*, 375 F. Supp. 1354, 1355 (N.D. Cal. 1974) (concluding that extension telephone is not intercepting device under Title III) with *United States v. Harpel*, 493 F.2d 346 (10th Cir. 1974) (holding that surreptitious recording of private conversation by use of extension telephone violated Title III).

39. 375 F. Supp. 1354 (N.D. Cal. 1974).

40. *Christman*, 375 F. Supp. at 1355 (noting that Congress intended to apply criminal sanctions to certain interceptions of communications).

41. *Id.*

42. *Id.*; see *supra* note 26 and accompanying text (defining base violation under 18 U.S.C. § 2511(1)(a) as actual or attempted willful interception of any "wire or oral communication").

43. *Christman*, 375 F. Supp. at 1355.

44. *Id.*

telephone without a court order,<sup>45</sup> allowing him to pick up and monitor calls on the "closed dial" system.<sup>46</sup>

The district court, in finding the defendant not guilty of illegal wiretapping, drew a number of conclusions regarding the scope of Title III. First, the court focused on the statutory reference to "common carrier" facilities in § 2510(1).<sup>47</sup> Relying on the legislative history of Title III, the court concluded that the statute was not intended to cover "privately operated intercommunication" systems, but rather only systems that are provided by a common carrier would be subject to Title III.<sup>48</sup>

Second, the court focused on the "oral" communications provisions of Title III, and noted that such communications are protected only where the speaker is demonstrating a reasonable expectation of privacy.<sup>49</sup> The court gauged the reasonableness of the privacy expectation by the employee's improper use of the telephone, concluding that it would be unreasonable for employees "misusing a private telephone system" to expect "that the communication is not subject to interception."<sup>50</sup>

Finally, the court looked to the language of § 2510(5)(a) of Title III<sup>51</sup> and concluded that an extension telephone is not an intercepting device within the meaning of the statute.<sup>52</sup> The district court wasted few words explaining this view,<sup>53</sup> evidently relying on its view of the section's plain language. Thus, in accordance with §

---

45. See 18 U.S.C. § 2511(2)(a)(ii)(A) (1988) (prescribing that providers of wire or electronic communication service are authorized to intercept wire, oral, or electronic communications if such provider has court order to do so).

46. *Christman*, 375 F. Supp. at 1355; see also *United States v. Blattel*, 340 F. Supp. 1140, 1142 (N.D. Iowa 1972) (holding that first essential element of Title III violation is wire communication utilizing facilities of common carrier); *ELECTRONIC SURVEILLANCE*, *supra* note 21, at 37 (stating that private carrier communications systems are not within definition of "wire communication" under Title III).

47. *Christman*, 375 F. Supp. at 1355.

48. *Id.*

49. *Id.*

50. *Id.*

51. 18 U.S.C. § 2510(5) of the 1968 version of Title III provided that an "[e]lectronic, mechanical, or other device" includes any apparatus that can be used to intercept a wire or oral communication, "except (a) any telephone . . . instrument, equipment or facility, or any component thereof, (i) being furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business." *Id.* This language has been termed the "business extension exception" and requires that (1) the extension telephone have been provided to the user by a communications common carrier in the ordinary course of that carrier's business, and (2) that the recipient of the extension telephone have used it in a manner consistent with the ordinary course of its business. *Id.*

52. *Christman*, 375 F. Supp. at 1355.

53. *Id.* (dismissing claim that extension telephone can be intercepting device in single sentence).

2510(5)(a), an extension telephone provided by a communications common carrier in the ordinary course of business, which is used by the subscriber in the ordinary course of business, is incapable of being an "intercepting device."<sup>54</sup>

*b. Other court decisions*

In *Campiti v. Walonis*,<sup>55</sup> decided in 1979, the First Circuit Court of Appeals flatly rejected the conclusion reached in *Christman* that there existed an "extension telephone" exception to liability under § 2510(5)(a).<sup>56</sup> The Tenth Circuit, in *United States v. Harpel*,<sup>57</sup> also rejected the *Christman* approach, concluding that the surreptitious recording of a private conversation with an extension telephone violated the spirit and purpose of Title III, which was the protection of privacy.<sup>58</sup> The courts' disparate application of the provisions of Title III did not go unnoticed by congressional observers.<sup>59</sup> Over time, the statute underwent numerous modifications,<sup>60</sup> but it was not

54. *Id.* The result in *Christman* came about because at the time Title III was enacted there were few private carriers. See S. REP. NO. 541, *supra* note 17, at 2-3, reprinted in 1986 U.S.C.C.A.N. at 3556-57 (discussing proliferation of companies offering telecommunications services following AT&T divestiture and deregulation). The provisions of Title III were aimed at protecting the privacy of an individual who was utilizing one of the public common carriers in existence at the time. Under § 2510(5)(a) of Title III, equipment provided to the subscriber by a communications common carrier, and used in the subscriber's ordinary course of business, did not satisfy the definition of an intercepting device. See *infra* notes 86-88 and accompanying text (discussing pre-ECPA "extension telephone exception").

55. 611 F.2d 387 (1st Cir. 1979).

56. *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979) (basing its conclusion on purpose of statute, which is to prohibit unlawful monitoring and, as such, nature of equipment used to conduct such monitoring should not be part of inquiry).

57. 493 F.2d 346 (10th Cir. 1974).

58. See *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974) (holding that telephone extension used without authorization or consent to surreptitiously record private telephone conversations is not used in ordinary course of business).

59. See S. REP. NO. 541, *supra* note 17, at 2, reprinted in 1986 U.S.C.C.A.N. at 3556 (citing statement of Senator Leahy that pre-ECPA Title III was "hopelessly out of date").

60. The first set of amendments were in 1970. See Pub. L. No. 91-358, tit. II, § 211(a), 84 Stat. 654 (1970) (adding § 2511(2)(a)(ii) relating to telephone company assistance in wiretapping); Pub. L. No. 91-452, tit. III, § 227(a), 84 Stat. 930 (1970) (deleting § 2514 relating to immunity); Pub. L. No. 91-452, tits. VIII, IX, XI, §§ 810, 902(a), 1103, 84 Stat. 940, 947, 959 (1970) (adding obstruction of state or local law enforcement, gambling, and racketeering offenses to crimes encompassed by § 2516(1)(c)); Pub. L. No. 91-452, tit. IX, § 902(b), 84 Stat. 947 (1970) (expanding scope of permissible disclosure under § 2517(3)); Pub. L. No. 91-358, tit. II, § 211(b), 84 Stat. 654 (1970) (authorizing orders compelling telephone company assistance in § 2518(4)); Pub. L. No. 91-358, tit. II, § 211(c), 84 Stat. 654 (1970) (expanding good faith defense of § 2520 to include reliance on legislative authorization).

The 1971 amendment, Pub. L. No. 91-644, tit. IV, § 16, 84 Stat. 1891 (1971), added assaults, and other attacks on members of Congress, the Cabinet, and the Supreme Court to the crimes encompassed by § 2516(1)(c).

The 1978 amendments, Pub. L. No. 95-511, tit. II, § 201(a)-(d), 92 Stat. 1796, 1797 (1978), deleted § 2511(3), which related to national security surveillance and amended §§ 2511(2)(a)(ii), 2518(4), 2518(9), 2518(10)(a), and 2519(3) to conform to the Foreign

until the substantial 1986 amendments that Congress significantly addressed the risk of private employer interceptions of employee communications using emerging technologies.<sup>61</sup>

### *B. The Electronic Communications Privacy Act of 1986*

By 1985, the telecommunications landscape had changed dramatically from that of Title III's original 1986 enactment.<sup>62</sup> Both the communications technology and the means of electronic surveillance experienced a revolution.<sup>63</sup> In response to this new technological topography, Congress instructed the congressional Office of Technology Assessment (OTA) to perform a study and report on "technological developments in the basic communication and information infrastructure of the United States that present new or changed opportunities for and vulnerabilities to electronic surveillance."<sup>64</sup> Focusing on new developments in wire and electronic communications, the OTA found that revolutionary changes to the U.S. tele-

---

Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811 (1988). In addition, Pub. L. No. 95-598, tit. III, § 314(h), 92 Stat. 2677 (1978) conformed language in § 2516(1)(c) regarding bankruptcy fraud to reflect amendments to the bankruptcy laws.

The 1982 amendments, Pub. L. No. 97-285, §§ 2(e), 4(e), 96 Stat. 1220, 1221 (1982) conformed § 2516(1)(c) to amendments to 18 U.S.C. §§ 351, 1751, which related to assaults and other attacks on government officials.

The 1984 amendments, Pub. L. No. 98-473, § 1203, 98 Stat. 2152 (1984), (1) added the Deputy Attorney General and Associate Attorney General to the list of officials who may be specially designated to approve applications for surveillance orders under § 2516(1), and request for emergency surveillance under § 2518(7); (2) added fraud by wire, radio, or television, witness tampering and retaliation, and sexual exploitation of children to the crimes encompassed by § 2516(1)(c); and (3) added the immediate danger of death or serious physical injury to the circumstances in which emergency surveillance can be conducted under § 2518(7) (*cited in* JAMES G. CARR, *THE LAW OF ELECTRONIC SURVEILLANCE* § 2.3, at 2-7 to 2-8 nn.28-28.1 (1993)).

61. The 1986 amendments, Pub. L. 99-508, 100 Stat. 1848 (1986), extended the coverage of Title III to electronic communications, cellular telephones, and data transmissions, added or altered definitions to correspond with the expanded coverage, added new penalty provisions, increased the range of offenses that can be investigated by a Title III order, and made several procedural changes in the statute. Provisions were also added to regulate the use of pen registers and trace devices, and the acquisition of toll records. *See generally* S. REP. NO. 541, *supra* note 17, at 11-50, *reprinted in* 1986 U.S.C.A.N. at 3565-3604 (providing detailed analysis of modifications made to Title III by ECPA).

62. *See* H.R. REP. NO. 647, *supra* note 7, at 17-18 (stating that pre-ECPA Title III failed to anticipate advent of "text, digital or machine communication" and increasing use of communications that are not routed through communications common carriers, such as E-mail, videotex, and other private services).

63. *See* ELECTRONIC SURVEILLANCE, *supra* note 21, at 3. An OTA study begins by asserting that "[a]dvances in electronics, semiconductors, computers, imaging, data bases, and related technologies have greatly increased the technical options for surveillance activities." *Id.* Further, the OTA suggested that the advent of cordless telephones, electronic mail, and pagers are vulnerable to monitoring, and that Title III came into being at a time when "electronic surveillance was limited primarily to simple telephone taps and concealed microphones (bugs)." *Id.*

64. ELECTRONIC SURVEILLANCE, *supra* note 21, at iii.

phone system, as well as the introduction of electronic services such as E-mail, fell outside the scope of Title III.<sup>65</sup> This shortfall was primarily due to the fact that these new methods of communication are not "aurally acquired," thus making the current law obsolete.<sup>66</sup>

Congress responded to the recognized deficiencies of Title III by introducing the Electronic Communications Privacy Act of 1986 (ECPA).<sup>67</sup> The ECPA was intended to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies," and to offset the fact that the existing Title III was "hopelessly out of date."<sup>68</sup>

### 1. *Expanded coverage of the ECPA*

The most comprehensive amendments to Title III added by the ECPA focused on the definitions contained in § 2510.<sup>69</sup> Of these changes, one of the most significant was the addition of § 2510(12), adding and defining "electronic communication."<sup>70</sup> The phrase is defined very broadly,<sup>71</sup> and encompasses any communication "not carried by sound waves and [those that] cannot fairly be categorized as containing the human voice."<sup>72</sup> Further, the term "electronic

---

65. The OTA study presented a litany of communications services that evolved after enactment of Title III, including satellite, digital switching, cellular, cordless telephones, electronic mail, computer, and electronic bulletin boards. All of these were beyond the scope of pre-ECPA Title III. ELECTRONIC SURVEILLANCE, *supra* note 21, at 3.

66. See ELECTRONIC SURVEILLANCE, *supra* note 21, at 3 (stating that Title III protection has "not kept pace with these technological changes"). The OTA study noted that the pre-ECPA Title III protected "only conversations . . . capable of being heard by the human ear." *Id.* at 19-20. This reasoning was echoed by Congress when it considered the ECPA. See S. REP. NO. 541, *supra* note 17, at 1, reprinted in 1986 U.S.C.C.A.N. at 3556 (stating that pre-ECPA Title III is "expressly limited to the unauthorized aural interception of wire or oral communications. It only applies where the contents of a communication can be overheard and understood by the human ear."); H.R. REP. NO. 647, *supra* note 7, at 18-19 (recognizing that data transmissions cannot be "aurally intercepted," which is predicate to violation of pre-ECPA Title III).

67. S. REP. NO. 541, *supra* note 17, at 1, reprinted in 1986 U.S.C.C.A.N. at 3555.

68. S. REP. NO. 541, *supra* note 17, at 1-2, reprinted in 1986 U.S.C.C.A.N. at 3555-56.

69. The ECPA amended § 2510 to include definitions for "electronic communication," "electronic communications system," "electronic communications service," "electronic storage," and "aural transfer." S. REP. NO. 541, *supra* note 17, at 14, reprinted in 1986 U.S.C.C.A.N. at 3568.

70. *Id.* The addition of "electronic communication" to Title III opened the door for the protection of a host of modern communications technologies not covered prior to 1986. See *id.* (noting that addition of electronic communications into statute now provides protection to communications not "carried by sound waves").

71. "Electronic communication" is defined 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." 18 U.S.C. § 2510(12) (1988).

72. S. REP. NO. 541, *supra* note 17, at 14, reprinted in 1986 U.S.C.C.A.N. at 3568.

communication" was inserted in the statute wherever Title III had previously referenced only wire and oral communications.<sup>73</sup>

In addition, the legislative history of the ECPA's amendment to § 2510(1) makes it clear that Congress intended to expand Title III to cover not only interceptions of communications sent via common carriers, but also to private telephone networks.<sup>74</sup> Congress also rewrote the definition of "intercept" found at § 2510(4). Under the old Title III definition, "intercept" encompassed only the aural acquisition of a wire or oral communication.<sup>75</sup> Thus, only sound-producing communications could be intercepted.<sup>76</sup> The ECPA revised the definition of "intercept" to include both "aural" and other means of acquiring wire, oral, or electronic communications.<sup>77</sup> The express intent of Congress in amending the definition of "intercept" was to bring "electronic" communications within the purview of Title III and to provide protection for the "non-voice portion of a wire communication."<sup>78</sup>

---

73. See 18 U.S.C. § 2510(4) (adding "electronic" to "wire" and "oral" communications included in definition of "intercept"); 18 U.S.C. § 2511(1)(a) (adding "electronic" communications, in addition to "wire" and "oral," to base offense).

74. See S. Rep. No. 541, *supra* note 17, at 3, *reprinted* in 1986 U.S.C.C.A.N. at 3556-57 ("It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute."). Section 2510(1) was modified by changing the language from "any person engaged as a common carrier in providing or operating such facilities" to "any person engaged in providing or operating such facilities." The deletion of the common carrier requirement allowed Congress to bring private telephone systems within the ambit of Title III. It also removed the primary basis for the district court's holding in *United States v. Christman*, 375 F. Supp. 1354 (N.D. Cal. 1974), indicating that the ECPA would have brought about a different result in that case.

75. See *supra* note 66 and accompanying text (discussing applicability of pre-ECPA Title III only to communications that could be aurally acquired).

76. See *supra* notes 42-54 and accompanying text (discussing holding of *Christman*).

77. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988 & Supp. V 1993)). Because Title III applies only to the interception of communications, "intercept" is one of the more critical operative terms in the statute for determining whether a violation has occurred. If the activity in question does not involve interception, as defined by § 2510(4), Title III is inapplicable, although constitutional restraints may still apply to the particular activity without reference to Title III. As amended in 1986, § 2510(4) defines "interception" 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). The legislative history to the 1986 amendments states that the addition of the reference to "other" acquisition (in addition to aural) is intended to make clear that "it is illegal to intercept the non-voice portion of a wire communication, such as the digitized portion of a voice communication." See S. REP. NO. 541, *supra* note 17, at 12, *reprinted* in 1986 U.S.C.C.A.N. at 3566; H.R. REP. NO. 647, *supra* note 7, at 34.

78. S. REP. NO. 541, *supra* note 17, at 13, *reprinted* in 1986 U.S.C.C.A.N. at 3567.

To further expand the protections of the ECPA, Congress added a new title, § 2701, covering "stored communications."<sup>79</sup> Under its provisions, any party who "(1) intentionally accesses without authorization a facility through which an electronic communication is provided; or (2) intentionally exceeds an authorization to access that facility . . . while it is in electronic storage" may be subject to both fines and imprisonment as provided in § 2701(b).<sup>80</sup> Finally, Congress amended § 2511, concerning the interception of wire, oral, or electronic communications, by increasing the minimum damages award a plaintiff may receive from \$1000 to \$10,000,<sup>81</sup> and added a new civil damages provision to create a private right of action for violation of the stored communications provisions of § 2701.<sup>82</sup>

## 2. Retention of pre-ECPA statutory exceptions

While the post-ECPA Title III does protect many forms of commu-

---

79. 18 U.S.C. § 2701 (1988). Title II of the ECPA established guidelines for the protection of stored communications, with the intended goal of addressing the rising problem of unauthorized parties gaining access to private wire and electronic communications. See Pub. L. No. 99-508, 1986 U.S.C.C.A.N. at 3589.

80. 18 U.S.C. § 2701(a). The ECPA added a definition of "electronic storage" at § 2510(17). Electronic storage is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17)(A)-(B).

Although the primary focus of the stored communications provisions was the protection of E-mail, the reference to stored wire communications in § 2510(17) indicates that voice mail was considered to be within the purview of this section. See H.R. REP. NO. 647, *supra* note 7 at 63 (discussing ECPA, and stating that both E-mail and voice mail are subject to general prohibitions added by § 2701). The Senate Report on the ECPA appears to take a somewhat different view of voice mail, stating that the ECPA amendments "specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly." S. REP. NO. 541, *supra* note 17, at 12, *reprinted in* 1986 U.S.C.C.A.N. at 3566. This disparity is significant because the degree of privacy protection afforded wire and electronic communications appears to differ based on whether the communication is being transmitted, and thus protected under § 2511 of the ECPA, or in electronic storage, which subjects the communication to § 2701 protection. The variable protection offered by these two provisions is discussed in greater detail *supra* note 70 and accompanying text.

81. See Pub. L. No. 99-508, 100 Stat. 1848, 1854 (codified at 18 U.S.C. § 2520) (reviewing amended civil remedies available pursuant to ECPA). Section 2520, as amended, included (1) declaratory or equitable relief; (2) damages consisting of the greater of a plaintiff's actual damages and "any profits the violator made as a result of the violation" or "statutory damages" of either \$100 per day or \$10,000, whichever is greater; and (3) reasonable attorney's fees and litigation costs. *Id.*

82. *Id.*, 100 Stat. at 1860 (codified as amended at 18 U.S.C. § 2701). New § 2707 included: (1) declaratory or equitable relief as appropriate; (2) damages consisting of "actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation," with a minimum recovery of \$1000; and (3) reasonable attorney's fees and litigation costs. *Id.* It is evident from the civil damages provisions that the minimum amount of civil damages prescribed for violations of stored communications are substantially less than those available for a wrongful interception of wire, oral, or electronic communications. This suggests a congressional intent to provide a lower degree of protection to stored communications, although no such intent is explicit in the legislative history.



nication that previously lacked a legal shield, the ECPA retained or redefined many of the statutory provisions existing prior to the 1986 amendments, which provided employers with broad authority to monitor employee communications.

a. *"Extension telephone" and "ordinary course of business" exceptions*

In the ECPA, Congress amended the definition of the term "intercept" to encompass acquisitions other than aural acquisitions and to include electronic communications in addition to wire and oral communications.<sup>83</sup> Further, Congress amended the scope of an intercepting device to include those capable of intercepting electronic communications.<sup>84</sup> While adding to the scope of protected communications with one hand, Congress legislatively took away those protections with the other.<sup>85</sup> This is most apparent in the modifications made by the ECPA to what is commonly termed the "extension telephone exception."<sup>86</sup> Under the pre-ECPA Title III,<sup>87</sup> an extension telephone used to monitor the telephone call of another party was arguably not an intercepting device if provided by a communications common carrier in the ordinary course of business and used by the subscriber in a manner consistent with the uses of an extension telephone in the ordinary course of business.<sup>88</sup> With the enactment

---

83. *Id.*, 100 Stat. at 1849 (codified at 18 U.S.C. § 2511). The statute reads in pertinent part: "'intercept' means 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) (1988).

84. Pub. L. No. 99-508, 100 Stat. at 1849 (codified at 18 U.S.C. § 2510(5)).

85. For example, the ECPA added to the list of protected communications those transmitted electronically, and provided a broadly inclusive definition of such communications. At the same time, however, Congress minimized the scope of this inclusion by retaining and expanding the language of § 2511(2)(a)(i), which prevents the provider of a wire or electronic communication service from being culpable for violations of the general liability provisions of § 2511(1). See 18 U.S.C. § 2511(2)(a)(i).

86. See *Briggs v. American Air Filter Co.*, 630 F.2d 414, 415 (5th Cir. 1980).

87. For examples of pre-ECPA judicial applications of the "telephone extension exemption," compare *United States v. Christman*, 375 F. Supp. 1354 (N.D. Cal. 1974) (holding that random monitoring of conversation over privately operated communications system is not forbidden by ECPA) and *United States v. Harpel*, 493 F.2d 346 (10th Cir. 1974) (finding that acquisition of content of telephone conversation through telephone equipment used in ordinary course of business was not unlawful) with *Briggs v. American Air Filter Co.*, 630 F.2d 414 (5th Cir. 1980) (holding that supervisor who listened to employee's conversation did so in ordinary course of business) and *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) (holding that personal call may be intercepted in ordinary course of business to determine nature, though never content).

88. 18 U.S.C. § 2510(5)(a)(i) (1982), as amended, 18 U.S.C. § 2510(5)(a)(i) (1988); see also *Christman*, 375 F. Supp. at 1355 (holding, in part, that extension phone used to monitor employee misconduct, which has been provided to subscriber by communications common carrier as part of its regular business, and is used in ordinary course of business by subscriber, cannot be intercepting device under Title III). Not all courts agree with the *Christman* holding

of the ECPA, the requirement that the "intercepting device" have been provided by a communications common carrier<sup>89</sup> was replaced by a more easily satisfied requirement that the "intercepting device" be furnished by "a provider of wire or electronic communication service in the ordinary course of its business" and used by the subscriber "in the ordinary course of its business."<sup>90</sup> This change brought private telephone networks within the scope of the exception, and arguably allows the owners of private networks to escape liability for monitoring employee telephone calls.

*b. System provider exception*

The ECPA amended § 2511(2)(a)(i) in a manner similar to § 2510(5)(a)(i), expanding its scope to include private communication networks.<sup>91</sup> This change allows an employee of a business with a private communications system to intercept other employees messages, so long as doing so is within the normal course of the employee's employment<sup>92</sup> and the interception occurs either as a

that the "device" aspect is dispositive of whether or not a violation of the statute has occurred. The First Circuit Court of Appeals in *Campiti v. Walonis* rejected the holding in *Christman* and argued that the applicability of Title III "should not turn on the type of equipment that is used, but whether the privacy of telephone conversations has been invaded in a manner offensive to the words and intent of the Act." *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979). The ECPA has not helped to eliminate the focus on the "device" issue. Rather, the "business extension" exception remains intact, and now applies to either wire or electronic communications services where both the installation and the use of the equipment are deemed to be in the ordinary course of business.

89. 18 U.S.C. § 2510(5)(a)(i) (1988).

90. *Id.* One pair of commentators, in reviewing whether the "intercepting device" or the circumstances surrounding the interception should be the focus of the inquiry, has argued that the better approach is to determine whether the intercepting device was used in a manner consistent with the subscriber's ordinary course of business. Barnett & Makar, *supra* note 24, at 726. These commentators rejected a result that would allow an employer to indiscriminately monitor employee telephone communications and yet avoid liability under Title III merely because the monitoring device was an extension telephone.<sup>2</sup> *Id.*

91. Pub. L. No. 99-508, 100 Stat. 1848, 1851 (codified as amended at 18 U.S.C. § 2511(2)(a)(i) (1988)). Section 2511(2)(a)(i) substituted "a provider of wire or electronic communication service" for "any communication common carrier." 18 U.S.C. § 2511(2)(a)(i). This ECPA exception for private communications providers contemplates a limited right to intercept or otherwise use electronic messages:

It shall *not be unlawful* under this chapter for an . . . officer, employee, or agent of a provider of [an] electronic communication service . . . 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.

*Id.* (emphasis added). Thus, if in a business context, an employee acts to intercept a message outside the scope of the intercepting employee's job duties, or if the interception is not necessary and incidental to providing the wire or electronic communications service or to protecting the employer's property rights in the system, the interception is not protected by the ECPA.

92. Pub. L. No. 99-508, 100 Stat. at 1851 (codified as amended at 18 U.S.C. § 2511(2)(a)(i)).

result of a necessary activity or occurs as a result of protecting the provider's rights or property.<sup>93</sup>

The ECPA also retained language in § 2511(2)(a)(i) expressly prohibiting the provider of *wire* communication services to the public from routine observation or random monitoring of communications except for "mechanical or service quality control checks."<sup>94</sup> No such bar exists for *electronic* communications systems.<sup>95</sup> Congress' failure to limit routine observation and random monitoring with respect to electronic communications systems may have been intentional.<sup>96</sup> This variation in treatment appears predicated on the belief that electronic communications services had a greater need for such observation and monitoring as a means to properly route message traffic.<sup>97</sup> Thus, § 2511(2)(a)(i) leaves E-mail messages susceptible to random interception, and accordingly more vulnerable to privacy invasions than voice mail messages.<sup>98</sup>

---

93. 18 U.S.C. § 2511(2)(a)(i); see also S. REP. NO. 541, *supra* note 17, at 20, *reprinted in* 1986 U.S.C.C.A.N. at 3574.

94. 18 U.S.C. § 2511(2)(a)(i). The legislative history to this section explained that electronic communications services may be subject to forms of system monitoring that are deemed necessary to the proper functioning of the service because such monitoring does not involve "human listening in on voice conversations." S. REP. NO. 541, *supra* note 17, at 20, 1986 U.S.C.C.A.N. at 3574. This is distinguished from similar monitoring of wire communications, which remained expressly prohibited by § 2511(2)(a)(i). *Id.*

95. S. REP. NO. 541, *supra* note 17, at 20, *reprinted in* 1986 U.S.C.C.A.N. at 3574.

96. See S. REP. NO. 541, *supra* note 17, at 20, *reprinted in* 1986 U.S.C.C.A.N. at 3574 (noting in legislative history of ECPA that random service monitoring of electronic communications systems is justifiable, as opposed to similar service monitoring of wire communications, which is not justifiable).

97. The legislative history of the ECPA specifically addresses this point:

In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone [wire] service. The provider of electronic communications services may have to monitor a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain.

S. REP. NO. 541, *supra* note 17, at 20, *reprinted in* 1986 U.S.C.C.A.N. at 3574.

One member of the popular press has arrived at a similar conclusion:

It's illegal for an employer to listen in on a person's telephone conversations even if those conversations take place on a company-owned phone. But there are no such clear privacy rules for the electronic mail that moves on a company's computer network. The major problem with offering privacy on a computer network is that a network administrator needs to have total access in order to properly maintain it.

Stephen C. Miller, *Privacy in E-Mail? Better to Assume It Doesn't Exist*, N.Y. TIMES, June 7, 1992, § 3, at 8.

98. The Senate report on the ECPA suggests that the dichotomy between potentially protected voice mail messages and unprotected E-mail messages may have been intentional. The legislative history categorizes voice mail as a wire communication protected under the ECPA. S. REP. NO. 541, *supra* note 17, at 12, *reprinted in* 1986 U.S.C.C.A.N. at 3556. When a voice mail message is stored, it retains the inherent character of a wire communication. The Senate determined that "wire" communications include "digitized communications to the extent that they contain the human voice at the point of origin, reception, or some point in between." *Id.* at 3566. The legislative history further states that "[a] private telephone system established by a company whose activities affect interstate commerce, would also be covered." *Id.* In

*c. Exceptions under the stored communications provisions*

During its consideration of the ECPA, Congress stated that the stored communications provisions were intended to address "the growing problem of unauthorized persons deliberately gaining access to, or sometimes tampering with, [stored] electronic or wire communications."<sup>99</sup> Congress nonetheless added language that appears to broadly protect the providers of stored electronic or wire communications systems from liability for accessing such systems.<sup>100</sup> It remains to be seen to what degree courts will bar employer liability based on this subsection.

## II. STATUTORY EXCEPTIONS FOR PRIVATE EMPLOYERS

There are relatively few cases interpreting Title III and the ECPA amendments in the employer-monitoring context. This is most likely a result of alternative avenues of redress, such as common law and state privacy statutes.<sup>101</sup> To date, all the federal court cases that have considered the issue are based on telephone-system monitoring.<sup>102</sup> Further, the vast majority were decided under the pre-ECPA

---

comparison, the legislative history indicates that the provider of an electronic communications service will not be liable for accessing stored communications on the system it has provided. *Id.* at 3590. Thus, a voice mail message, classified as a wire communication, bears an apparently greater degree of ECPA protection than does an E-mail message. The legislative history is silent as to the purpose of distinguishing between the two.

99. S. REP. NO. 541, *supra* note 17, at 35, *reprinted in* 1986 U.S.C.A.N. at 3589.

100. 18 U.S.C. § 2701(c)(1) (1988). This section states that accessing stored wire or electronic communications will not be unlawful if the system is accessed pursuant to authorization "by the person or entity providing a wire or electronic communications service." *Id.* This provision has not been tested in the courts, and commentators disagree about its scope. *See Hernandez, supra* note 19, at 39 (arguing that language of § 2701(c)(1) allows provider of E-mail or voice mail system to access all stored messages without risk of liability). *But see Baumhart, supra* note 19, at 925-26 (noting that at least one commentator views § 2701(c)(1) "as a blanket license for employers to peruse and disclose employee E-mail communications transmitted through company-owned systems," but countering that employers should not rely too heavily on this language given clear congressional intent to strengthen individual privacy rights through enactment of ECPA).

101. *See supra* note 16 (discussing various state causes of action that mirror Title III).

102. *See Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir. 1990) (holding that landlord did not violate Title III because tenant consented to interception of incoming telephone calls); *Campiti v. Walonis*, 611 F.2d 387, 392 (1st Cir. 1979) (holding that police officer's interception of inmates' telephone conversations was unlawful); *Kratz v. Kratz*, 477 F. Supp. 463, 467 (E.D. Pa. 1979) (stating that Title III did not exempt interspousal telephone interceptions). The federal courts have not yet decided a case brought pursuant to the wiretap statutes by an employee against an employer for unlawfully accessing that employee's E-mail or voice mail accounts pursuant to the wiretap statutes. There are, however, several lower court cases pending, or on appeal, in California for employer accessing of E-mail messages. Most of these claims are based on state privacy law. *See Cameron v. Mentor Graphics*, No. 716361 (Cal. Sup. Ct., Santa Clara Cty., filed Nov. 7, 1991) (claiming wrongful termination resulting from employer reading employee E-mail, where employer apparently searched employee's E-mail for sole purpose of finding incriminating information to support just-cause termination action, allowing

Title III.<sup>103</sup> These decisions reflect two analytical approaches to deciding whether to impose employer liability under Title III. In one set of cases, the courts emphasized that a legitimate business purpose<sup>104</sup> justified the employer monitoring. The other cases focus on the subject matter of the call as supporting the employer's interest in monitoring.

A. "*Legitimate Business Purpose*" Cases

*United States v. Harpel*<sup>105</sup> involved the criminal provisions of Title III.<sup>106</sup> Harpel, a former police officer, was charged with disclosing the contents of telephone conversations between other officers that had been unlawfully taped.<sup>107</sup> There was no evidence as to who made the tapes, and the police station where the tapes were evidently made possessed numerous telephone extensions, making such a determination difficult.<sup>108</sup> Nevertheless, Harpel was convicted of disclosing the contents of unlawfully intercepted wire communications

---

employer to avoid its contractual promise to honor stock options); *Bourke v. Nissan Motor Co.*, No. YC003979 (Cal. Sup. Ct., Los Angeles Cty., filed 1989); *Flanagan v. Epson America*, No. BC007036 (Cal. Sup. Ct., Los Angeles Cty., filed 1989). One case brought under California Penal Code § 631, was recently dismissed when the presiding judge found that the provision covered only telegraph interception and telephone wiretapping, but not electronic communications such as E-mail. Metz, *supra* note 19, at 26 (citing *Shoars v. Epson Am.*, No. SCW112749 (Cal. Sup. Ct., Los Angeles Cty., filed 1989)); cf. *supra* note 16 (comparing state wiretapping statutes providing private right of action and noting that some states provide protection only for oral or wire communications, while other states protect electronic communications in addition to wire and oral communications).

103. See, e.g., *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 584 (11th Cir. 1983) (holding that employer's monitoring policy must not extend beyond what was necessary to determine that call was personal); *Briggs v. American Air Filter Co.*, 630 F.2d 414, 420 (5th Cir. 1980) (concluding that manager's monitoring of phone call between employee and competitor was within ordinary course of business); *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974) (holding that telephone extension used without consent to surreptitiously record private conversation is not within ordinary course of business); *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 393-94 (W.D. Okla. 1978) (finding telephone company's monitoring activities were not unlawful interceptions because purpose was for quality control, employees knew of monitoring, and there were separate phones available for personal calls), *aff'd*, 611 F.2d 342 (10th Cir. 1979); *United States v. Christman*, 375 F. Supp. 1354, 1355 (N.D. Cal. 1974) (concluding that monitoring and recording conversations over department store's privately operated intercommunications system, after notice of improprieties occurring in store, was not unlawful interception); *United States v. Blattell*, 340 F. Supp. 1140, 1142 (N.D. Iowa 1972) (holding telephone company not guilty of unlawful wiretapping because prosecution failed to prove telephone company was common carrier and operating facilities for transmission of interstate or foreign communications).

104. This framework looks at whether: (1) the employer had a reasonable business justification for the intrusion; (2) employees were provided notice of the possibility of monitoring; and (3) the employer acted consistently with respect to the extent of monitoring of which employees were warned.

105. 493 F.2d 346 (10th Cir. 1974).

106. *United States v. Harpel*, 493 F.2d 346, 348 (10th Cir. 1974).

107. *Id.*

108. *Id.*

under 18 U.S.C. § 2511(1)(a).<sup>109</sup> On appeal to the Tenth Circuit, Harpel argued that it was likely that the conversation was recorded via an extension telephone and, therefore, based on the telephone extension exception, he could not be found liable.<sup>110</sup> The Tenth Circuit rejected Harpel's theory as too rigid an interpretation of the statutory exemption.<sup>111</sup> Instead, the court focused on the privacy rights at the heart of Title III, holding 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."<sup>112</sup> Thus, such conduct was not immune under Title III.<sup>113</sup>

In *James v. Newspaper Agency Corp.*,<sup>114</sup> the Tenth Circuit once again considered the applicability of the "extension telephone" exception, but in the context of employer telephone monitoring with a goal of helping employees provide better service to the public.<sup>115</sup> In *James*, a former employee of the Newspaper Agency Corporation sued under Title III, claiming that her calls had been unlawfully intercepted.<sup>116</sup> The court, in finding that the employer was not liable, emphasized that employees were provided with advance notice of the monitoring, the installation of the monitoring equipment was not performed secretly, and no employee protested the installation at the time it occurred.<sup>117</sup> Based on this reasoning, the court held that the employer's monitoring fell "squarely within" the ordinary course of business exception of § 2510(5)(a).<sup>118</sup>

The District Court for the Western District of Oklahoma reached a similar conclusion in *Simmons v. Southwestern Bell Telephone Co.*<sup>119</sup> In that case, the plaintiff was a former employee of Southwestern Bell who responded to customer service calls placed through a central switchboard.<sup>120</sup> The calls were routinely monitored by supervisory personnel to ensure quality control and to minimize personal use of

---

109. *Id.*

110. *Id.* at 351.

111. *Id.*

112. *Id.*

113. *Id.* Thus, not only would the party intercepting and recording the telephone conversation be liable under Title III, but also any party disclosing the contents of the recorded conversation. *Id.* at 348-49.

114. 591 F.2d 579 (10th Cir. 1979).

115. *James v. Newspaper Agency Corp.*, 590 F.2d 579, 581-82 (10th Cir. 1979).

116. *Id.*

117. *Id.* at 581.

118. *Id.*

119. 452 F. Supp. 392 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

120. *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 393 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

the lines.<sup>121</sup> After being fired for placing personal calls, the plaintiff sued, claiming that Southwestern Bell had violated Title III by monitoring his calls.<sup>122</sup> The court held that Southwestern Bell was not liable because there was a written policy, of which all the employees were aware, that prohibited personal use of the service telephones.<sup>123</sup> Further, Southwestern Bell maintained separate telephones for employee personal calls, which were not monitored, and the plaintiff had previously been warned to cease using the service telephones for personal calls.<sup>124</sup> The court concluded that the defendant's conduct was within both the letter and the spirit of Title III's authorization of telephone interceptions.<sup>125</sup>

### B. "Subject of the Call" Cases

Decisions falling within the "subject of the call" rubric focus on the specific content of the monitored telephone calls, and establish the basic rule that calls relating to the business of the employer may be intercepted. Thus, intercepting such calls is within the ordinary course of business and is legal. On the other hand, personal calls cannot be intercepted, except to the extent necessary to determine whether or not the call is personal.<sup>126</sup>

In *Watkins v. L.M. Berry & Co.*,<sup>127</sup> the Eleventh Circuit focused on the subject matter of a monitored conversation in determining whether an employer was liable under Title III.<sup>128</sup> At the time of the interception giving rise to the suit, Watkins was employed as a telephone sales representative for L.M. Berry & Company.<sup>129</sup> The company maintained a policy of monitoring employee sales calls over a standard extension telephone<sup>130</sup> as part of its on-going training program.<sup>131</sup> Employees were permitted to use their business tele-

---

121. *Id.*

122. *Id.* at 394. The plaintiff sought damages for his alleged wrongful termination. *Id.*

123. *Id.* at 396.

124. *Id.* The court did note, however, that if Southwestern Bell had monitored employee calls placed on the telephones designated for private use, then the court "would wholeheartedly agree that [Bell] had overstepped its limited privilege." *Id.*

125. *Id.* at 397.

126. The problems with this approach become readily apparent. For instance, if a personal call may be monitored only to the extent necessary to determine that it is personal in nature, what is a reasonable amount of time for an employer to monitor a call and determine it is, in fact, personal? Further, what are the employer's duties should the call be both personal and business-related in nature? The cases that accompany this discussion do not answer these questions.

127. 704 F.2d 577 (11th Cir. 1983).

128. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582-83 (11th Cir. 1983).

129. *Id.* at 579.

130. *Id.*

131. *Id.*

phones for personal calls, and were told by the company that personal calls would not be monitored, except to the extent necessary to determine whether the call was personal.<sup>132</sup>

The telephone call that gave rise to this suit was a personal call received by Watkins during her lunch break.<sup>133</sup> During this call, Watkins discussed a job interview she recently had with another company.<sup>134</sup> Unbeknownst to Watkins, the call was being monitored by her supervisor.<sup>135</sup> Shortly thereafter, Watkins was summoned to her supervisor's office, and when she realized that her call had been monitored an argument ensued, after which she was fired.<sup>136</sup>

L.M. Berry & Company argued that the supervisor's monitoring was not unlawful under Title III because Watkins knew that the company monitored calls and thus had consented to the interception.<sup>137</sup> The court quickly dispensed with that theory, stating that the general policy of monitoring business calls did not in any way serve as consent to monitor personal calls.<sup>138</sup> According to the court, to the extent that Watkins did consent to the monitoring of personal calls, she had done so in accordance with the company's own policy, which allowed for monitoring only to the degree necessary to determine that the call was personal.<sup>139</sup>

The company also argued that an extension telephone is not an "intercepting device" under Title III.<sup>140</sup> Rejecting that contention, the court found that the issue was not whether the extension was an "intercepting device," but rather whether the interception was made in the ordinary course of the company's business.<sup>141</sup> In holding that it was not, the court explained that (1) the call to Watkins had been in-coming, and thus could not have been a sales call, (2) the caller was a personal friend, and (3) the subject matter was personal in nature.<sup>142</sup> The Eleventh Circuit also affirmatively concluded that a personal call may not be intercepted in the ordinary course of business as prescribed by § 2510(5)(a)(i), except to the extent necessary to determine whether a call is personal or to prevent the

---

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.* at 580.

138. *Id.* at 581-82.

139. *Id.*

140. *Id.* at 580-81.

141. *Id.* at 582.

142. *Id.*



misuse of the company's telephone system.<sup>143</sup>

In *Epps v. St. Mary's Hospital of Athens*,<sup>144</sup> the plaintiffs were employees of St. Mary's Hospital, working as emergency medical technicians.<sup>145</sup> The hospital maintained a dispatching console that received in-coming calls and from which out-going calls could be placed.<sup>146</sup> These calls were automatically recorded.<sup>147</sup> Calls placed within the confines of the hospital were also routed through the console, but were not automatically recorded.<sup>148</sup>

At issue in the case was the recording of a personal call between the plaintiffs, placed between two points within the hospital facility.<sup>149</sup> In the call, the appellants made disparaging comments about hospital supervisory personnel that were later disclosed.<sup>150</sup> The technicians sued for actual and punitive damages under Title III.<sup>151</sup> They argued that the hospital was not protected by the "extension telephone" exception because the recording of the call was not in the ordinary course of the hospital's business.<sup>152</sup> The hospital argued that the recording was within the ordinary course of its business because the subject of the call concerned matters of employee relations, which were of importance to the hospital.<sup>153</sup>

Relying on *Watkins*, the court agreed with the hospital, stating the general rule that "if the intercepted call was a business call," then the "monitoring of it was in the ordinary course of business."<sup>154</sup> The

---

143. *Id.* The court stated that the phrase "in the ordinary course of business" does not mean anything that is of interest to a company. *Id.* The company's interest in *Watkins*' plans for other employment did not equate to a legitimate legal interest. *Id.* The court went on to note that for a private right of action to exist under Title III, it is unnecessary for the offender to hear anything in particular. Rather, all that is required is that the "listening in" take place. *Id.* at 582-84. Finally, the Eleventh Circuit concluded that even if the employer were to legitimately monitor an employee's call, that is, if the subject matter of the call were related to the employer's business, this does not mean that the entire call loses privacy protection under Title III. *Id.* at 584. If the call should turn to matters of a personal nature, the employer is obligated to cease monitoring even where the original monitoring would be immunized as in the ordinary course of business. *Id.* This analysis reflects the difficulty courts confront in determining whether the duration of an employer's monitoring was reasonable to decide if a call was of a personal nature. Judge Smith in the *Watkins* case stated that something less than three minutes would seem appropriate. *Id.* at 584 n.10.

144. 802 F.2d 412 (11th Cir. 1986).

145. *Epps v. St. Mary's Hosp. of Athens*, 802 F.2d 412, 413 (11th Cir. 1986).

146. *Id.*

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.* at 413-14. There is no indication in the court's opinion that the plaintiffs were terminated or disciplined for statements made during their conversation.

151. *Id.* at 413.

152. *Id.* at 416.

153. *Id.*

154. *Id.*

court held that where the call (1) "occurred during office hours," (2) "between co-employees," (3) "over a specialized extension which connected the principal office to a substation," and (4) "concerned scurrilous remarks about supervisory employees in their capacities as supervisors" the call was business in nature.<sup>155</sup> The court noted specifically that issues involving employee relations implicated the legal interests of the hospital.<sup>156</sup>

The Fifth Circuit Court of Appeals addressed a similar problem in *Briggs v. American Air Filter Co.*<sup>157</sup> In *Briggs*, one of the plaintiffs was a former salesman of defendant American Air Filter.<sup>158</sup> The other plaintiff worked for a competing business, yet maintained close contact with the employee of the defendant.<sup>159</sup> A manager at American Air Filter's Atlanta office, suspecting that his employee might be disclosing sensitive business information to the other company, listened in on a telephone conversation between the two, over an extension telephone.<sup>160</sup> The conversation included topics related to American Air Filter's business.<sup>161</sup>

The plaintiffs filed suit under Title III, and it fell to the court to determine whether American Air Filter was entitled to protection under the "extension telephone" exception.<sup>162</sup> Despite the fact that the plaintiffs had no advanced notice of the possibility of monitoring, the court held that American Air Filter was protected.<sup>163</sup> The court based this conclusion on a number of factors. First, the plaintiffs admitted that the call was related to American Air Filter's business.<sup>164</sup> Second, the actual monitoring took place only long enough to confirm the suspicions of the company.<sup>165</sup> Third, the specific act

---

155. *Id.* at 417.

156. *Id.* Judge Phyllis Kravitch, concurring in part and dissenting in part, noted that Congress enacted Title III to punish and deter eavesdropping, not to focus on the conduct of the person subject to the eavesdropping. *Id.* (Kravitch, J., concurring in part and dissenting in part) (disagreeing with majority's reliance on employees' conduct and conversation to determine whether employer's actions were in ordinary course of business). She argued that the intent of Congress was not to divide conversations into "protected and unprotected categories." *Id.* Instead, for the "extension telephone" exception to apply, the call must be more than merely related to business, but must advance a legitimate business purpose, and this purpose must exist at the time the monitoring takes place. *Id.* at 417-18.

157. 630 F.2d 414 (5th Cir. 1980).

158. *Briggs v. American Air Filter Co.*, 630 F.2d 414, 415-16 (5th Cir. 1980).

159. *Id.* at 416.

160. *Id.*

161. *Id.*

162. *Id.* at 417.

163. *Id.* at 420.

164. *Id.*

165. *Id.*

at issue was not part of a general policy of monitoring.<sup>166</sup>

In the more recent case of *Deal v. Spears*,<sup>167</sup> a court again faced the problem of determining the applicability of the "extension telephone" exception to employer monitoring.<sup>168</sup> The plaintiff was an employee in the defendant Spear's liquor store.<sup>169</sup> In response to a burglary of the store, Spears installed a recording device on an extension telephone to record all in-coming and out-going calls from the store, believing that an employee was involved in the theft and hoping that any incriminating statements made over the store telephone would be recorded.<sup>170</sup> The defendant recorded calls for a two month period, and the plaintiff was terminated based on the contents of a call that indicated she sold liquor at a reduced price, against store policy.<sup>171</sup> Although no evidence of complicity in the theft was garnered, many of the calls recorded involved "sexually provocative" discussions between the plaintiff and another party with whom she was having an extramarital affair.<sup>172</sup> The plaintiff brought a civil suit under § 2520 of Title III.<sup>173</sup>

Spears argued that the plaintiff had implicitly consented to the monitoring and recording, or, in the alternative, his conduct was protected by the "extension telephone" exception.<sup>174</sup> The court rejected any notion that the plaintiff had consented to the monitoring, as demonstrated by the nature of her conversations, which clearly indicated that she had no knowledge that the telephone was, or could be, monitored.<sup>175</sup> With respect to the "extension telephone" exception, the court turned to the Eleventh Circuit's holding in *Watkins*, concluding that a personal call may be intercepted in the ordinary course of business to determine its nature, but never its contents.<sup>176</sup> Because the defendant had intentionally recorded all calls, regardless of their nature, took no steps to limit the monitoring, and taped and disclosed calls that served no legitimate business

---

166. *Id.* The court noted the importance of the legitimate business purpose as a justification for the interception, and stated that under less compelling circumstances the employer might be required to show that prior warnings had been made to employees. *Id.* at 420 n.9.

167. 980 F.2d 1153 (8th Cir. 1992).

168. *Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992).

169. *Id.* at 1155.

170. *Id.* at 1155-56.

171. *Id.* at 1156.

172. *Id.* at 1155. The contents of the various recorded calls led Senior District Court Judge Harris to dub this a "case of sex, lies and audio tapes." *Deal v. Spears*, 780 F. Supp. 618, 620 (W.D. Ark. 1991), *aff'd*, 980 F.2d 1153 (8th Cir. 1992).

173. *Deal*, 980 F.2d at 1155.

174. *Id.* at 1156-57.

175. *Id.* at 1157.

176. *Id.* at 1158.

purpose, he was not entitled to the protection of the statutory exception.<sup>177</sup>

### III. THE STATUTORY FRAMEWORK MEETS THE MODERN TECHNOLOGIES

To assess the likelihood that office technologies such as E-mail and voice mail would be protected under the post-ECPA Title III, it is necessary to draw analogies to the cases applying the statute to extension telephones. Additionally, it is important to understand the variations in the statutory protection provided to electronic and wire communications in the transmission phase, and the same communications once stored.

#### A. *Comparing the Cases to E-mail and Voice Mail*

As the case law suggests, employees have no automatic right to, or expectation of, privacy when using their employer's telephone.<sup>178</sup> At the same time, certain circumstances make it unlawful for an employer to listen in on an employee's telephone conversations, even when those conversations take place on company-owned equipment.<sup>179</sup> What this has come to mean, through the defining process of litigation, is that under Title III employers cannot deliberately monitor an employee's personal calls unless they fall within one of the statutory exceptions.<sup>180</sup>

As discussed in Part II, the cases applying Title III to telephone systems reflect two possible approaches to determining employer liability: whether the employer has a legitimate business purpose for monitoring, and whether the subject matter of the communications is inherently protected. Either approach may protect communications via voice mail or E-mail systems, depending on the circumstances.

Assuming a court focused on content, then the general rule of the *Epps*, *Watkins*, *Briggs*, and *Deal* line of cases would apply. As a general

---

177. *Id.* The district court awarded the plaintiff \$40,000 in statutory damages and attorney's fees pursuant to § 2520(c)(2)(B), but denied their request for punitive damages. *Deal*, 780 F. Supp. at 624-25. On appeal, although the Eighth Circuit concluded that the scope of the eavesdropping went far "beyond the boundaries of the ordinary course of business," *Deal*, 980 F.2d at 1158, the court held that the employers' violations of Title III did not warrant the imposition of punitive damages because the violations were not wanton, reckless, or malicious. *Id.* at 1159.

178. *See supra* note 103 and accompanying text (addressing limited scope of employee privacy recognized by case law).

179. An employer can only monitor an employee's telephone call to determine its nature, but never its contents. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 583 (11th Cir. 1983) (finding employer justified in listening to call to determine whether call was personal or business).

180. *See Deal*, 780 F. Supp. at 622.

premise, a court would allow any business-related communication to be monitored because it implicates the legal and legitimate business interests of the employer.<sup>181</sup> By the same token, personal communications would be protected under Title III regardless of the circumstances, and could only be monitored to the extent necessary to determine that they are personal.<sup>182</sup> Thus, under the subject matter approach, E-mail and voice mail should receive the same degree of protection as telephonic communications.

The *James* and *Simmons* line of cases focuses, instead, on whether the employer has a legitimate business purpose for monitoring employee communications.<sup>183</sup> That employees were on notice of the possibility of monitoring, employers relied on a reasonable business justification for the monitoring, and actions by the employer were consistent with its monitoring policy are all dispositive proof that a legitimate business purpose exists. With respect to E-mail and voice mail systems, the subject matter approach should protect employee communications.

### B. Irrationality of Title III

Although Title III, as judicially interpreted, offers some minimal degree of employee privacy in E-mail and voice mail communications, such widely variable approaches in the application of Title III suggest significant weaknesses in the statutory construction. This is perhaps no more apparent than in the ECPA amendments that provide for differing levels of privacy protection for stored and non-stored communications.

The general prohibition against eavesdropping on wire, oral, or electronic communications addressed in § 2511(1)(a) protects such communications from "interception."<sup>184</sup> Although the definition of "intercept" found in § 2510(4) sets out the means by which a prohibited interception occurs,<sup>185</sup> it does not specify the temporal

---

181. As the Eleventh Circuit implied in *Watkins*, for an employer's interception of employee telephone communications to be protected under Title III, the employer must have a legal interest in that communication, not merely curiosity. *Watkins*, 704 F.2d at 582.

182. See *id.* at 583 (stating that "personal call may not be intercepted in the ordinary course of business under [Title III], except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not").

183. See *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979) (looking to purpose of employer monitoring to train employees in dealing with public and to protect employees from abusive customers); *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 393 (W.D. Okla. 1978) (focusing on employer monitoring as means to ensure service quality, to check work in progress, and to provide assistance to employees), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

184. 18 U.S.C. § 2511(1)(a) (1988).

185. *Id.* § 2510(4).

point at which an acquisition is in fact an "interception," and thus proscribed. Based on the common definition of "intercept," meaning to "interrupt the progress or course of,"<sup>186</sup> the acquisition of a wire, oral, or electronic communication will constitute an "interception," only while being transmitted in a manner prescribed by § 2511(1)(b)(i)-(iii).<sup>187</sup>

By contrast, the stored communications provisions of § 2701 prohibit the unauthorized accessing of wire or electronic communications once stored.<sup>188</sup> While the distinction between the terms "intercept" and "access" has little significance for forms of communication that only exist as transmissions, and are never stored, the distinction is critical when a transmitted communication is later electronically stored, because it is at the time of storage that a communication becomes subject to different provisions of the ECPA. This is the case with both E-mail and voice mail messages,<sup>189</sup> both of which have a transmission phase and a storage phase.<sup>190</sup> During the transmission phase, any protection against unlawful interception under Title III is governed by § 2511.<sup>191</sup> On arrival in storage, the same messages are subject to § 2701.<sup>192</sup> Thus, the same message is subject to differing standards of protection merely because it exists in a different statutorily defined medium.

This conclusion identifies a particularly irrational result in the employer monitoring context. Under § 2511(1)(a) an employer, even if the owner and provider of the communications system, is limited in the extent to which employee communications can be intercepted while being transmitted. The federal case law considering telephone systems clearly establishes a framework in which employer monitoring is and is not permissible. On the other hand, § 2701(c)(1) appears

---

186. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1986). "Intercept" derives from the Latin word *intercipere*, meaning to seize in transit. *Id.* Compare the term "access," which is defined as "a way by which a thing . . . may be reached." *Id.* at 11.

187. 18 U.S.C. § 2511(1)(b)(i)-(iii).

188. *Id.* § 2701(a)(1) (barring unauthorized intentional accessing of stored electronic communications).

189. The Office of Technology Assessment report that preceded and precipitated the ECPA amendments to Title III noted that electronic mail exists at five discrete stages: "(1) at the terminal or in the electronic files of the sender, (2) while being communicated, (3) in the mailbox of the receiver, (4) when printed into hardcopy before mailing, and (5) when retained in the files of the electronic mail company for administrative purposes." ELECTRONIC SURVEILLANCE, *supra* note 21, at 45. Similarly, voice mail starts its journey as a wire communication, but becomes a stored communication once recorded.

190. See *supra* notes 7-8 (discussing basic E-mail and voice mail technology respectively).

191. See *supra* notes 69-82 and accompanying text (discussing amendments made to Title III by enactment of ECPA).

192. See *supra* note 79 and accompanying text (discussing ECPA amendment relating to "stored communications").

to grant the provider of the wire or electronic communications service blanket permission to monitor stored communications.<sup>193</sup> The provider in this context will almost certainly be the employer.<sup>194</sup> Thus, the limitations imposed on employer interceptions of wire or electronic communications vanish once the same communication is in storage. Accordingly, in order to avoid Title III liability, an employer need only access employee communications once they have been stored. This seems an insupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA.<sup>195</sup>

#### IV. RECOMMENDATIONS

Employees in the private sector are not protected by the Fourth Amendment.<sup>196</sup> Consequently, they must rely on other federal enactments, state statutes, or common law to ensure their privacy rights. While employers arguably need information about employees regarding their conduct and performance, this need must be balanced against employees' reasonable expectations of privacy.<sup>197</sup> The following discussion suggests ways for employers to balance their need for information with that of employee privacy rights.

##### A. *Employers*

Employers must strive to balance their legitimate, identifiable business needs against their employees' right to privacy and dignity in the workplace. Employers, however, can do much to minimize potential morale problems and legal challenges based on employee expectations of privacy in office communications by doing some basic review and planning in their personnel policies and procedures. The following suggestions are offered to assist employers in striking an appropriate balance between the needs of the business and the employee.

First, publish and post a policy defining the intended business uses

---

193. See *supra* note 72 and accompanying text.

194. In its consideration of the ECPA, Congress noted that the risks to communications privacy were, in part, the result of the growth in the development of private communications system by private companies. H.R. REP. NO. 647, *supra* note 7, at 18. Congress made this observation in 1986, and use of private communications systems has increased in the intervening years.

195. See *infra* note 207 and accompanying text (discussing significance of privacy considerations in passage of Title III and ECPA).

196. U.S. CONST. amend. IV; see also *United States v. Goldstein*, 532 F.2d 1305, 1311 (9th Cir.) (noting that Fourth Amendment is constraint on government action rather than actions of private individuals), *cert. denied*, 429 U.S. 960 (1976).

197. See Baumhart, *supra* note 19, at 939 (discussing balance between employees' privacy interest and reasonableness of employer's quality control search).

of E-mail and voice mail systems, and indicate that these systems may be accessed by the employer without notice to employees. Employees should be made aware that E-mail and voice mail are to be used for business purposes only, and that messages contained on these systems are considered to be company records. Employee awareness of the policy will minimize expectations of privacy and likely reduce the chance of a challenge.<sup>198</sup> The policy should clearly state the procedure that will be implemented by the company and the reason that such a policy is required. Further, the policy should specify the company's rationale for accessing employee E-mail or voice mail to prevent any inference that the company is engaging in "eavesdropping" without identifiable reasons. The company should promote the legitimate basis upon which a genuine need exists to access E-mail or voice mail records.

Second, inform employees of overall company privacy guidelines and establish a mechanism whereby complaints may be addressed. Third, clearly outline, to supervisors and managers, corporate expectations regarding employees' privacy in these systems. Further, the company should define the circumstances under which managers can search for, or interfere with, E-mail and voice mail messages. The E-mail and voice mail policies should address third-party access, for example, access by immediate supervisors or co-workers.

Finally, conduct periodic reviews of E-mail and voice mail systems to affirm that they are being used in accordance with the company's established guidelines. The policy should also establish guidelines for recording an employee's unauthorized use of such systems. Thus, employers seeking to discipline or terminate employees for such misuse will have documentation to support the employer's actions.

### *B. Statutory Reform*

The ECPA evolved from Congress' recognition of the inherent flaws in the outdated Title III of 1968. In the House report on the ECPA, the privacy of citizens was extolled as a key factor mandating passage. The report notes that if "Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right.

---

198. See, e.g., *United States v. Willoughby*, 860 F.2d 15, 19 (2d Cir. 1988) (finding that prison inmates' use of telephone constitutes implied consent to monitoring because inmates were warned their calls would be monitored); *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979) (noting that personnel were notified of telephone monitoring); *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 396 (W.D. Okla. 1978) (stating that telephone monitoring was reasonable when all employees knew and acquiesced to monitoring of phone calls), *aff'd*, 611 F.2d 342 (10th Cir. 1979).



Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."<sup>199</sup> Similarly, the Senate recognized in its report on the ECPA the implicit irrationality of the pre-ECPA Title III when it suggested that "[i]t does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute."<sup>200</sup> While both Houses explicitly recognized the importance of communications privacy in any context, for reasons that are not entirely clear, Congress stopped short of providing broad privacy protections to emerging technologies used in the private corporate environment. As was the case in 1986, Title III is again ripe for amending.<sup>201</sup>

First, Title III should be amended to account for the judicially defined conclusion regarding basic telephone systems; that is, employers cannot deliberately monitor an employee's personal communications that are made at work.<sup>202</sup> This is best achieved by adding explicit language that permits employer monitoring only where a legitimate business purpose can be demonstrated. The courts have shown a willingness to carve out a protected zone of private communications even in the workplace, and Title III should incorporate similar limitations on employer monitoring.

Second, Congress should amend the statute to remove the irrational distinction between the use of telephones, E-mail, and voice mail.<sup>203</sup> The congressional emphasis on privacy issues during consideration of the ECPA highlights the importance of protecting the message, not the medium. There is no practical reason why these

---

199. H.R. REP. NO. 647, *supra* note 7, at 19.

200. S. REP. NO. 541, *supra* note 17, at 3, *reprinted in* 1986 U.S.C.C.A.N. at 3556-57.

201. In 1993, Congress sought to address the vulnerability of U.S. workers to privacy intrusions from their employers by introducing the Privacy for Consumers and Workers Act, S. 984, 103d Cong., 1st Sess. (1993); H.R. 1900, 103d Cong., 1st Sess. (1993).

Although the Act would not have prohibited employers from accessing employee E-mail and voice mail accounts, it would require employers to provide written notice to employees subjected to electronic monitoring. S. 984 at 7-8; H.R. 1900 at 6-7. Although intended to prevent employer's abuses of electronic monitoring in the workplace, the Senate bill was never forwarded from the Subcommittee on Employment and Productivity of the Senate Committee on Labor and Human Resources and the House bill was never acted upon by the House Committee on Education and Labor after having been forwarded to the full committee from the Subcommittee on Labor-Management Relations.

202. See *supra* notes 128-43 and accompanying text (discussing *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983), which established notion that employer may listen to employee's telephone calls to determine subject, but never content).

203. See *supra* notes 184-95 and accompanying text (comparing variable protection provided by ECPA to E-mail and voice mail communications).

technologies should be treated differently. Whether a message is "intercepted," "accessed," or "acquired" should be irrelevant to an employer's liability, and employee communications should be protected regardless of whether the message is transmitted or remains in storage.

Finally, the statutory exception for communications system providers should be curtailed or eliminated. The current statutory language has changed little since the passage of Title III in 1968, and reflects a communications environment dominated by common carriers. The exception as originally enacted was intended to protect common carriers from liability while in the normal provision of service.<sup>204</sup> This is clearly no longer the case, nor is the business communications market now dependent on major carriers.<sup>205</sup> This exception should not be extended to corporate providers of communications services to employees. Rather, only where a corporation is able to demonstrate a legitimate business purpose for monitoring employee communications should it be protected from liability.

### CONCLUSION

The legislative history of the ECPA highlights the importance of individual privacy concerns as a primary reason for bringing E-mail, voice mail, and other forms of previously unprotected communications under the umbrella of Title III.<sup>206</sup> The Senate Report notes one's interest in the privacy of correspondence does not change based on the form the correspondence takes.<sup>207</sup> Clearly, the medium is not the message. In passing Title III and amending it with the ECPA, however, Congress has created a dual standard that provides

---

204. See Burnside, *supra* note 7, at 464-65 (discussing exemption of common carriers from ambit of Title III).

205. See *supra* note 174 and accompanying text (discussing profusion of private communications systems at time of ECPA's passage).

206. The intent of Congress to take account of privacy concerns is further evidenced by incorporation into the ECPA the Office of Technology Assessment's most rigorous recommendations respecting telephone and electronic communications. In its study, the OTA suggested three options for congressional consideration regarding telephone surveillance: (1) extending the protection of Title III to all telephone communications regardless of the transmission technology (analog, digital, cellular, or cordless); (2) formulating specific policies depending on the technological constraints and possibilities; and (3) taking no action whatsoever and allowing the courts to define the appropriate level of privacy protection. ELECTRONIC SURVEILLANCE, *supra* note 21, at 38. With respect to electronic communications such as E-mail, the OTA offered Congress three options, again ranging from protecting such communications at all phases of transmission and storage, to taking no action at all. *Id.* at 51. With respect to both wire and electronic communications, Congress adopted the more stringent of the OTA-proffered options. See generally Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988 & Supp. V 1993)).

207. S. REP. NO. 541, *supra* note 17, at 5, reprinted in 1986 U.S.C.C.A.N. at 3559.

inadequate protection against private employer incursions into employee communications. Congressional action is again necessary to clarify the privacy protections established by Title III. To leave forms of telecommunications technology unprotected merely because they are newly developed and more advanced than earlier technology is not in accord with the purpose of Title III. To permit minuscule technological differences to be dispositive of Title III's protection is inimical to its intent. The legislative history of Title III is replete with expressions of concern for privacy interests,<sup>208</sup> and it is in consideration of these privacy concerns that Title III again merits revision.

---

208. See S. REP. NO. 1097, *supra* note 24, at 66, *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153; S. REP. NO. 541, *supra* note 17, at 5, *reprinted in* 1986 U.S.C.C.A.N. at 3559; *see also* Gelbard v. United States, 408 U.S. 41, 48 (1972) (stating that protection of privacy was major concern in congressional passage of Title III); *Zweibon v. Mitchell*, 606 F.2d 1172, 1182 (D.C. Cir. 1979) (noting that dominant purpose of Title III was to prevent improper privacy invasions), *cert. denied*, 453 U.S. 912 (1981).

