PEEK AND SPY: A PROPOSAL FOR FEDERAL REGULATION OF ELECTRONIC MONITORING IN THE WORK PLACE

INTRODUCTION

In 1987, the Office of Technology Assessment reported that employers were electronically monitoring more than six million employees in the work place.[1] Electronic monitoring is most prevalent in industries which rely on the telephone to conduct business. These industries include: telemarketing, customer service, airline reservations and telephone operators.[2] Employers use electronic monitoring devices primarily to evaluate employee performance, increase productivity, provide security for employer property and investigate misconduct.[3] However, federal and state wiretapping laws may impose civil or criminal liability on employers who choose to monitor employees either overtly or covertly.[4]

Title III of the Omnibus Crime Control and Safe Streets Act ("Title III") regulates electronic monitoring.[5] In 1968, Congress enacted Title III to protect the privacy of wire and oral communications, and to authorize the interception of wire and oral communications in certain circumstances.[6] Although section 2511 of Title III prohibits any electronic interception of a wire, oral or electronic communication,[7] it contains two statutory exceptions applicable to employee monitoring in the work place: the business-extension exception and the consent exception.

---

1. Office of Technology Assessment, OTA-LIT-333, *The Electronic Supervisor: New Technology, New Tensions*, 5 (1987) [hereinafter *OTA Report*].

2. Daily Lab. Rep. (BNA), Sept. 25, 1991, A-19.

3. *OTA Report*, *supra* note 1, at 91. Employers may also monitor to prevent employees from leaking industry secrets or committing acts for which a court could hold the employer vicariously liable. *See* John P. Furfaro & Maury B. Josephson, *Electronic Monitoring in the Workplace*, N.Y. L.J., July 6, 1990, at 3.

4. *See* Kirk W. Munroe, *Commercial Eavesdropping: A Catch 22*, 63 FLA. B.J. 1, 11 (Mar. 1989) (arguing that a company which monitors to prevent employee misconduct potentially exposes itself to "lawsuits, penalties and damages").

5. 18 U.S.C. §§ 2510-2521 (1988). The Act is generally referred to as Title III.

The scope of communications covered by Title III includes wire, oral and electronic communications. Title III defines "electronic communications" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic or photoptical system that affects interstate commerce," but excludes cordless telephones, tone-only paging devices and tracking devices. 18 U.S.C. § 2510 (12) (1988).

6. S. REP. NO. 1097, 90th Cong., 2d Sess. 66, *reprinted in* 1968 U.S.C.C.A.N 2112, 2153 [hereinafter *1968 Senate Report*].

7. 18 U.S.C. § 2511(1) provides in part:

The business-extension exception allows an employer to monitor employees when a telephone or telegraph component used in the ordinary course of the business is the device which intercepts the communication.[8] Under the consent exception, an employer may electronically monitor employees who have previously consented to the monitoring.[9] Courts have struggled in applying both the business-extension and the consent exception.[10] The ambiguous judicial interpretations of these exceptions

---

(1) Except as otherwise specifically provided in this chapter any person who-

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

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication . . .

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

(d) intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

18 U.S.C. § 2511(1) (1988).

8. The business-extension exception is imbedded in the definition provisions of Title III. Under § 2511(1) of Title III, an "interception" of wire or oral communications must occur to establish an actionable violation. Section 2510(4) of Title III defines an "interception" as requiring the use of an "electronic, mechanical, or other device." Specifically, § 2510(4) provides: " 'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical, or other device . . ." 18 U.S.C. § 2510(4) (1988).

However, § 2510(5)(a)'s definition of "electronic, mechanical or other device" excludes an employer monitoring in the ordinary course of business.

18 U.S.C. § 2510(5)(a) provides:

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than-

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

18 U.S.C. § 2510(5)(a) (1988).

9. 18 U.S.C. § 2511(2)(d) provides:

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.

18 U.S.C. § 2511(2)(d) (1988).

10. Munroe, *supra* note 4, at 12-13.

may serve to impose civil or criminal liability on unknowing employers who electronically monitor employee actions.[11]

Illegal electronic monitoring constitutes a felony punishable by imprisonment for up to five years.[12] Section 2520 of Title III also creates a private right of action for injured parties.[13] Moreover, a court may require an employer engaging in illegal monitoring to pay damages to each party to the conversation.[14]

In addition to the legal exposure posed by the federal wiretapping statutes, state surveillance statues also regulate electronic monitoring. Based on the legislative history of Title III, courts have consistently held that state statutes may impose more restrictive provisions than those contained in Title III.[15] Only seven states have refused to enact statutes regulating electronic surveillance.[16] Consequently, a regional or national corporation that engages in employee monitoring could comply with fed-

---

11. *See id.* at 11 ("An employer must, therefore, traverse a legal mine filed in order to benefit from the advantages of commercial electronic surveillance.").

12. 18 U.S.C. § 2511(4)(a) (1988). First offenders who do not monitor for a tortious or illegal purpose or for commercial advantage or private commercial gain are subjected to either: (1) a fine of $500; or (2) imprisonment for one year and/or a statutory fine. 18 U.S.C. § 2511(4)(b) (1988). There is a mandatory statutory fine of $500 for second offenders. 18 U.S.C. § 2511(5)(a)(ii)(B) (1988).

13. 18 U.S.C. § 2520(a) provides in pertinent part:

> Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520(a) (1988).

Under § 2520, appropriate relief includes: equitable relief, damages, punitive damages in an appropriate case, and reasonable attorneys' fees. The statutory damages are computed by assessing the greater of $100 a day for each day of violation or a lump sum of $10,000. 18 U.S.C. § 2520(b), (c) (1988).

14. *See, e.g.,* Deal v. Spears, 780 F. Supp. 618 (W.D. Ark. 1991) (finding the two defendant-employers liable for statutory damages to both parties to the monitored conversations and mandating that each defendant pay each conversant $10,000).

15. *See, e.g.,* Navarra v. Bache Halsey Stuart Shields, Inc., 510 F. Supp 831, 833 (E.D. Mich. 1981). "The state statute must meet the minimum standards reflected as a whole in the proposed chapter. The proposed provision envisions that [s]tates would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation." *Id.* (citing S. REP. NO. 1097, 90th Cong., 2d Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2187).

16. The following states have not enacted wiretapping statutes: Alabama, Arkansas, Mississippi, Missouri, Montana, Tennessee, South Carolina and Vermont. Although South Carolina does not have a law generally prohibiting wiretapping, one South Carolina statute does regulate pen registers and trap devices. *See* S.C. CODE ANN. §§ 17-29-10 to 17-29-50 (Law. Co-op. 1990).

eral law but, at the same time, violate state law.[17]

Despite the existence of federal and state regulatory statutes, estimates suggest that employers currently monitor sixty-six percent of the computerized workforce.[18] In response to this evidence of pervasive monitoring in the work place, Congress recently introduced the Privacy for Consumers and Workers Act.[19] The drafters of this legislation intended the proposed Act "to prevent potential abuses of electronic monitoring" in the work place.[20]

Neither the proposed Act nor existing state or federal wiretapping legislation effectively satisfies the needs of both employers and employees. This Note argues that legislation granting employees affirmative rights in the work place will strike a better balance between employer and employee interests. Part I discusses the business-extension exception to Title III. Part II analyzes the consent exception to Title III. Part III examines the pertinent sections of the proposed Privacy for Consumers and Workers Act. Part IV criticizes Title III and the proposed Privacy for Consumers and Workers Act. Finally, Part V proposes federal regulation for employee monitoring in the work place.

I. THE BUSINESS-EXTENSION EXCEPTION

The business-extension exception arises from Title III's section 2510(5)(a). This section permits the interception of a communication where telephones or electronic communications systems used in the ordinary course of business serve as the intercepting device.[21] This exception does not require employee consent if the employer meets the statutory

17. Munroe, *supra* note 4, at 12. In addition, an employer doing business in more than one state could engage in conduct that is sanctioned by one state, but prohibited by another state. *Id.*

18. *The Privacy for Consumers and Workers: Hearings on H.R. 1218, Act Before the Subcomm. on Labor-Management Relations of the House Comm. on Education and Labor*, 102d Cong., 1st Sess. 2 (1991) [hereinafter *Hearings on H.R. 1218*] (statement of Hon. Pat Williams, Chairman) (citing statistics compiled by the National Institute for Occupational Safety and Health).

19. Senator Paul Simon (D-IL) introduced the Senate version of the Privacy for Consumers and Workers Act, S. 516, on February 27, 1991. Representative Pat Williams (D-MT) introduced the House version, H.R. 1218, on February 28, 1991.

20. H.R. 1218, 102d Cong., 1st Sess. (1991) [hereinafter H.R. 1218].

21. *See supra* note 9. Under Title III as enacted in 1968, the business-extension exception would not apply unless a communications common carrier furnished the telephone equipment to the subscriber. In 1986, Congress enacted the Electronic Communications Privacy Act of 1986 and amended § 2510(5)(a) to include equipment furnished by "a provider of wire or electronic communications services." Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(c)(4), 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2510(5)(a) (1988)).

requirements of section 2510(5)(a).[22] The business-extension exception, which originated in an early draft of Title III, contained a blanket exception for extension telephones.[23] Originally, Congress did not intend to regulate a normal extension telephone under Title III.[24] The version of Title III that Congress finally enacted expanded the exception to include "any telephone or telegraph instrument," but limited the exception's application to interceptions made in the ordinary course of business.[25] This limitation, coupled with the requirement that the employer use a "telephone or telegraph instrument" to monitor the work place, forms the basis of the business-extension exception.[26]

A. Type of Intercept

The business-extension exception only applies when the intercepting device utilized is telegraph or telephone equipment.[27] Originally, Title III protected only wire and oral communications from unauthorized interception.[28] However, advances in communications technology limited the applicability of Title III. Consequently, in 1986, Congress amended the statute by enacting the Electronic Communications Privacy Act, which brought electronic communications within the category of pro-

22. *See* Briggs v. American Air Filter Co., Inc., 630 F.2d 414, 419 (5th Cir. 1980) ("To hold that a business extension telephone is a[n] [electronic] 'device' unless it is used with the consent of one of the parties to the conversation would be to read the extension telephone exception out of the law, because 18 U.S.C. § 2511(2)(d) makes clear that interception is generally not unlawful if one of the parties to the communication has authorized the interception . . . We do not believe Congress intended the exception to be superfluous. . . .").

23. *Id.* at 418. The earlier draft of the bill stated: "The term 'electronic, mechanical or other device' does not include . . . an extension telephone instrument furnished to the subscriber or user by a communications common carrier in the ordinary course of its business." *Id.* (citing H.R. 5470, 90th Cong., 1st Sess., § 2515(d)(1) (1967), *reprinted in Hearings on the Anti-Crime Program Before the Subcomm. No. 5 of House Comm. on the Judiciary*, 90th Cong., 1st Sess. 892, 894 (1967)).

24. 630 F.2d at 418.

25. *Id.* Congress probably offered this limitation on the blanket exception in response to the testimony of Professor Herman Schwartz, who appeared before the House Judiciary Committee on behalf of the American Civil Liberties Union. Professor Schwartz testified that extension telephones could be used to invade someone's privacy. *Id.* (citing H.R. 5470, 90th Cong., 1st Sess. § 2515(d)(1) (1967), *reprinted in Hearings on the Anti-Crime Program Before the Subcomm. No. 5 of House Comm. on the Judiciary*, 90th Cong., 1st Sess. 892, 894 (1967)).

26. Section 2510(5)(a) of Title III only exempts "any telephone or telegraph instrument, equipment or facility, or any component thereof. . ." from the prohibition on wiretapping. *See supra* note 9.

27. 18 U.S.C. § 2510(5)(a).

28. 18 U.S.C. § 2511 (1982), *amended by* 18 U.S.C. § 2511 (1986).

tected communications.[29] Congress intended the Electronic Communications Privacy Act to bridge the gap between the 1968 Act and the development of new communications technology.[30] As amended, Title III now affords protection to any transfer of data by wire, radio or other electronic means.[31]

Although Title III prohibits unauthorized interception of electronic, oral and wire communications, the business-extension exception specifies that telephone or telegraph equipment must act as the intercepting device.[32] Courts have interpreted this language broadly to include a variety of communications systems.[33] Moreover, courts have held that where an employer records rather than monitors a particular telephone call, the telephone intercepts the call, not the recording device.[34] Although a re-

29. The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101, 100 Stat. 1848-53 (1986) (codified as amended at 18 U.S.C. § 2510(12) (1988)).

30. S. REP. No. 541, 99th Cong., 2d Sess. 9, *reprinted in* 1986 U.S.C.C.A.N. 3555 [hereinafter *1986 Senate Report*].

31. 18 U.S.C. § 2510(12) (1988). Specifically, advanced technological methods of communication now encompassed within the scope of Title III include: digital communications, data communications, video communications, electronic mail and communications via fiberoptic cable. Russell S. Burnside, Note, *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 (1987). Primarily, electronic communications were outside the scope of Title III prior to 1986 because Title III required that there be an aural interception in order to establish a violation. *See* 18 U.S.C. § 2510(4) (1982) (amended 1986). The 1986 Act merely amended the definition of "intercept" to include an "aural or other acquisition." 18 U.S.C. § 2510(4) (1988).

32. *See supra* note 9 and accompanying text.

33. An emergency dispatch console is an example of such a communication device. The console is a monitoring device placed on the phone by a telephone company and a police station telephone system.

In Epps v. St. Mary's Hosp., the Eleventh Circuit held that the statutory exception included an emergency dispatch console. 802 F.2d 412, 415 (11th Cir. 1986). Defendants monitored the telephone call in question by using an extension line of the hospital's dispatch console which the hospital used to receive emergency calls and dispatch emergency services. *Id.* at 413. The *Epps* court held that the dispatch console clearly fell within the statutory requirement. *Id.* at 415.

In James v. Newspaper Agency Corp., the Tenth Circuit held that the business-extension exception applied where the employer requested that the telephone company install a monitoring system to permit the supervisors to monitor employees. 591 F.2d 579, 581 (10th Cir. 1979).

In Jandak v. Village of Brookfield, 520 F. Supp. 815 (N.D. Ill. 1981), the court held that the exception included routine recording of emergency calls on a police station telephone system. *Id.* at 822.

34. *See* Royal Health Care Servs. v. Jefferson-Pilot Life Ins., 924 F.2d 215, 217 (11th Cir. 1991) (holding that under the Florida business-extension exception (which is identical to Title III's business-extension exception codified at 18 U.S.C. § 2510(5)(a)) the telephone extension is the device that intercepts the call because it can intercept a call without recording the call); *Epps*, 802 F.2d at 415 (11th Cir. 1986) (holding that the dispatch console was the intercepting device rather than the

cording device does not qualify for the statutory exception, if the employer connects the recording device to a telephone outlet, then the interception will fall within the exception.[35]

B. Ordinary Course of Business

An employer must intercept a communication in the ordinary course of business to fall within the business-extension exception. The legislative history of Title III provides no guidance as to what Congress intended by the "ordinary course of business" limitation.[36] Courts differ over the interpretation of the "ordinary course of business" clause with respect to two issues: surreptitious monitoring and monitoring personal telephone calls in the work place.

In *United States v. Harpel*,[37] the Tenth Circuit held that surreptitious monitoring violated the purpose of Title III and therefore did not fall within the ordinary course of business.[38] In *Harpel*, while at a local bar, a police officer played an unauthorized tape recording of a conversation between another police officer and a federal agent.[39] The Tenth Circuit

---

double reel tape recorder used to record the telephone calls); United States v. Harpel, 493 F.2d 346, 350 (10th Cir. 1974) ("[T]he recording of a conversation is immaterial when the overhearing is itself legal. . . It is the receiver which services this function [intercepting] — the recorder is a mere accessory designed to preserve the contents of the communication.").

35. *See* Abel v. Bonfanti, 625 F. Supp. 263, 270 (S.D.N.Y. 1985) (holding that the means of intercepting a communication are irrelevant as long as the employer attaches the device to an extension phone outlet, and intercepts the call in the ordinary course of business).

36. Briggs v. American Air Filter Co., 630 F.2d 414, 418 (5th Cir. 1980). The Senate Report omitted the business-extension exception from the list of exceptions outlined in the report. *Id.* at 414 (citing S. REP. No. 1097, 90th Cong., 2d Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153).

37. 493 F.2d 346 (10th Cir. 1974).

38. *Id.* at 351. However, the Tenth Circuit includes non-surreptitious monitoring within the ordinary course of business exception. In James v. Newspaper Agency Corp., the court held that non-surreptitious employee monitoring with prior written notice to employees falls within the employer's ordinary course of business. 591 F.2d 579, 581 (10th Cir. 1979). In *James*, the employer requested that the telephone company install a monitoring device to allow supervisors to train and instruct employees in dealing with the general public. *Id.* The monitoring was not surreptitious, and the employers provided the employees with advance notice of the policy. *Id.* In addition, the monitoring system protected employees from abusive telephone calls. *Id.* Concluding that the monitoring occurred in the ordinary course of business, the court also recognized the legitimate purposes for monitoring. *Id.*

39. 493 F.2d at 348. This case arose under the criminal provisions of Title III. Harpel was convicted of disclosing an unlawfully intercepted wire or oral communication in violation of 18 U.S.C. § 2511(1)(c). *Id.* Under this section, it is unlawful to disclose intentionally, or endeavor to disclose, the contents of any intercepted conversation where the party knows or has reason to know that the information was obtained through a violation of the wiretapping laws. 18 U.S.C. § 2511(1)(c) (1988).

held that unauthorized use of a telephone extension to surreptitiously monitor a private telephone conversation is not in the ordinary course of business.[40]

In contrast, the Fifth Circuit, in *Briggs v. American Air Filter Co.*,[41] held that under certain circumstances the ordinary course of business exception encompasses surreptitious monitoring. In *Briggs*, a supervisor suspected that an employee was discussing confidential business matters during a telephone call to a competitor.[42] The supervisor listened and recorded part of the telephone call using the extension telephone in his office.[43] The court ruled that the supervisor monitored the call during the ordinary course of business, because the supervisor had specific suspicions regarding the employee's conduct and listened only long enough to confirm his suspicions.[44] However, the court specifically declined to decide whether the ordinary course of business exception supported a general policy of surreptitious monitoring or authorized the interception of personal telephone calls.[45]

In 1983, in *Watkins v. L.M. Berry & Co.*,[46] the Eleventh Circuit became the first circuit court to consider whether the ordinary course of business exception permitted the interception of personal telephone calls. The court stated that although a business call is conclusively within the ordinary course of business exception, a personal call only qualified for the exception to the extent necessary to guard against unauthorized use of the telephone.[47] The court defined a business call as a telephone conversation in which the employer had a legal interest.[48] In *Watkins*, a supervisor intercepted an employee's telephone call in which the em-

40. 493 F.2d at 351. *See* Burnside, *supra* note 31, at 487 n.239. *See also* Campiti v. Walonis, 611 F.2d 387, 392 n.5 (1st Cir. 1979) (recognizing that "[t]he Senate Report declares that Title III created a flat ban on all unauthorized electronic surveillance," notwithstanding the extension telephone exception).

41. 630 F.2d 414 (5th Cir. 1980).

42. *Id.* at 416. Specifically, the supervisor suspected that the employee was disclosing the employer's job bid which the employer expected to submit the following day. *Id.*

43. *Id.* The supervisor recorded the call by using an attachment to a dictating machine. *Id.*

44. *Id.* at 420. The court declined to comment on the legality of the interception had the supervisor continued to intercept the entire telephone call. *Id.*

45. *Id.* The plaintiffs stipulated that the telephone call in question was a business rather than a personal call. Therefore, the court noted that it did not need to decide whether the ordinary course of business exception could ever include the interception of a personal telephone call. *Id.*

46. 704 F.2d 577 (11th Cir. 1983).

47. *Id.* at 582-83.

48. *Id.* at 582.

ployee discussed alternative employment opportunities.[49] The court held that the employee's telephone conversation constituted a purely personal call because the employer had no legal interest in the employee's future plans to interview for other employment positions.[50] Therefore, the court concluded that the employee's personal telephone call did not fall within the employer's ordinary course of business.[51]

Only three years later, the Eleventh Circuit applied the standard adopted in *Watkins* in *Epps v. St. Mary's Hospital of Athens, Inc.*,[52] and held that an employer has a legal interest in maintaining the job environment.[53] In *Epps*, a hospital employee overheard two other employees criticize hospital supervisors while speaking on the hospital's internal telephone line.[54] The employee recorded the conversation on the system used to record incoming emergency calls.[55] The *Epps* court determined that the telephone call was a business call because the call occurred during business hours, between employees, and concerned criticism of the employee's supervisors in a business capacity.[56] The court found that the employer had a legal interest in preventing contamination of the work place.[57] Thus, the court concluded that the call fell within the ordinary course of business exception.[58]

---

49. *Id.* at 579.

50. *Id.* at 582.

51. *Id.* The *Watkins* court stated that it could not expand "the phrase 'in the ordinary course of business' to mean anything that interests a company" because such a broad interpretation of the exception would "flout the words of the statute." *Id.* Further, the court acknowledged that if a situation ever existed in which an employer could monitor a personal call, then this constituted such a case because the employee discussed matters of great interest to the employer. *Id.* at 583. However, the court concluded that it is unacceptable to formulate a rule including the interception of personal telephone calls within the ordinary course of business. *Id.*

52. 802 F.2d 412 (11th Cir. 1986).

53. *Id.* at 416-17.

54. *Id.* at 413.

55. *Id.* at 413-14. The employee testified that she did not listen to the conversation as she recorded it. *Id.* at 418. Applying the business-extension exception to unauthorized monitoring by an employee, the Eleventh Circuit implicitly held that surreptitious monitoring may fall within the ordinary course of business.

56. *Id.* at 417.

57. *Id.* at 416-17.

58. *Id.* The dissent, however, argued that the majority incorrectly relied on the *Watkins* decision. *Id.* at 417. *Watkins* held that intercepting a call that is merely related to business does not advance a legitimate business purpose. *Id.* (citing *Watkins*, 704 F.2d at 582). The dissent stated that in this case no legitimate business purpose existed for the interception at the time the eavesdropping employee recorded the call. *Epps*, 802 F.2d at 418. Moreover, the dissent argued that an eavesdropper cannot evade the federal wiretapping provisions by claiming that her employer might be interested in the gossip of its employees. *Id.* The dissent reasoned that his interpretation of the

II. THE CONSENT EXCEPTION

Section 2511(2)(d) of Title III provides that a person not acting under color of law may intercept a communication where the person is either a party to the conversation, or where one of the parties to the conversation has given prior consent to the interception.[59] Under the consent exception, an employer may monitor the communications of employees who have given "prior consent" to the interception.[60] Beyond indicating that consent may be express or implied, the legislative history offers little indication of the intended scope of "prior consent."[61] Courts disagree, however, on the extent to which a court should infer consent in a case lacking the presence of express consent.[62] Moreover, in adopting a case-by-case approach, courts have failed to establish a framework for evaluating the scope of consent.[63]

In *Watkins v. L.M. Berry & Co.*,[64] the Eleventh Circuit narrowly interpreted the scope of both express and implied consent. In *Watkins*, an employee brought a Title III suit against her employer for wrongfully intercepting a personal telephone call.[65] The employee consented to the employer's policy of generally monitoring business calls, but only monitoring personal telephone calls to the extent necessary to ensure that a

record suggested that the eavesdropper fished for material that he could use to fire the two parties to the conversation. *Id.* The wiretapping statute "does not immunize busybodies and malicious gossips." *Id.*

59. 18 U.S.C. § 2511(2)(d) (1988). An employer invokes the consent exception by requiring employees to sign a consent form which indicates that the employee is consenting to the interception of communications by someone not a party to the conversation.

60. The first clause of § 2511(2)(d), which allows a party to a conversation to monitor the conversation, does not apply in the situation of an employer monitoring an employee. 18 U.S.C. § 2511(2)(d) (1988).

61. The legislative history notes that "[s]urveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to." *1968 Senate Report*, *supra* note 6, at 2182.

62. The legislative history of Title III indicates that the consent exception merely reflects prior existing law. The legislative history demonstrates an assumption that consent of one party will mitigate any interception of a wire, oral or electronic communication. *Id.* The paucity of legislative history regarding the consent exception as applied in the workplace is attributable to the primary purpose of Title III. Congress intended Title III to regulate the use of wiretapping and electronic surveillance in the administration of justice. *Id.* at 2113.

63. Munroe, *supra* note 4, at 12 ("The primary lesson of *Watkins* is that every interception will be evaluated separately to determine whether consent was obtained.").

64. 704 F.2d 577 (11th Cir. 1983).

65. *Id.* at 579. The supervisor monitored a telephone call in which the employee discussed an employment interview with another company and indicated a strong interest in accepting a position with that company. *Id.*

particular conversation was a personal call.[66] The *Watkins* court noted that the employee did not expressly consent to the monitoring of her personal call by the employer because she only consented to the limited monitoring of her business calls.[67] The court held that Title III did not preclude the employee from limiting the extent of her consent.[68] The court concluded that the trier of fact must determine whether the scope of the employee's consent encompassed the particular monitored call at issue.[69]

In the absence of express consent, the *Watkins* court considered whether an employee could imply consent. The employer argued that the employee impliedly consented to the interception by accepting employment after receiving actual notice of the monitoring policy.[70] The Eleventh Circuit concluded that "consent under Title III is not to be cavalierly implied."[71] Consequently, the court held that an employee's mere knowledge of an employer's monitoring capability does not constitute implied consent.[72]

Declining to follow *Watkins*, the Second Circuit, in *United States v. Amen*,[73] held that the legislative history of Title III indicates that Congress intended courts to interpret the consent exception broadly.[74] In *Amen*, two inmates argued that they did not consent to the monitoring of their telephone calls by prison officials, even though all of the inmates received notice of monitoring.[75] The *Amen* court concluded that if a

66. *Id.* Berry Company's business consisted primarily of telephone solicitation. *Id.* The company hired and trained Watkins to solicit current and prospective advertisers by telephone. Berry Company monitored the telephone solicitation calls as part of its employee training program. *Id.* The calls were monitored by a standard extension telephone that was located in the supervisor's office. The supervisor would later review monitored calls with the employee and discuss how to improve sales techniques. *Id.*

67. *Id.* at 581. The employee consented only to the inadvertent interception of a personal call. Watkin's supervisor disregarded this policy by intercepting a substantial portion of her conversion. *Id.*

68. *Id.* at 582.

69. *Id.*

70. *Id.* at 581.

71. *Id.* The court noted that it would thwart Title III's purpose of protecting individual privacy to routinely imply consent from certain circumstances. *Id.*

72. *Id.* The court focused on the fact that Watkins relied on a scheme of limited monitoring. *Id.*

73. 831 F.2d 373 (2d Cir. 1987). The potential illegality of the interception arose in the context of a criminal defendant's motion to suppress the wiretap evidence as unlawfully obtained. *Id.* at 378.

74. *Id.* (citing S. REP. No. 1097, 90th Cong., 2d Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182).

75. *Id.* at 379. This case arose under 18 U.S.C. § 2511(2)(c) rather than § 2511(2)(d). *See*

party to a conversation receives actual notice of monitoring, and disregarding that notice places a call on the monitored telephone, then he is deemed to have impliedly consented to the monitoring.[76]

In *Griggs-Ryan v. Smith*,[77] the First Circuit followed the Second Circuit's analysis in *Amen*, acknowledging that Congress intended a broad interpretation of the consent requirement.[78] The *Griggs* court found that an individual implies consent where the circumstances indicate that the party knowingly agreed to the monitoring.[79] In *Griggs*, a tenant claimed that he did not consent to the landlord's interception of a personal telephone call, even though the landlord repeatedly warned the tenant that she recorded all incoming calls.[80] The court concluded that the tenant impliedly consented to the interception because he continued to speak freely on the monitored telephone line even after receiving actual notice of the landlord's monitoring.[81] Declining to formulate a test for

---

supra note 9 for the text of § 2511(2)(d). Section 2511(2)(c) is nearly identical to § 2511(2)(d), except that it provides a consent exception for a person acting under color of law.

Section 2511(2)(c) provides in pertinent part:

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

18 U.S.C. § 2511(2)(c) (1988).

76. 831 F.2d at 379. The court found that the inmates received actual notice of the prison's policy of monitoring telephones from at least four sources. *Id.* First, the Code of Federal Regulations provided that there is a possibility of monitoring prison telephones. *Id.* Second, upon arriving at the prison, each inmate attended a lecture in which prison officials discussed the monitoring policy. *Id.* Third, each prisoner received an informational handbook containing a notice regarding the monitoring system. *Id.* Finally, prison officials placed notices on each telephone. *Id.*

77. 904 F.2d 112 (1st Cir. 1990).

78. *Id.* at 116.

79. *Id.* at 116-17. The court noted that circumstances relevant to determining whether implied consent exists include language or acts which indicate that the party "knows of, or assents to, encroachments on the routine expectation that conversations are private." *Id.* at 117.

80. *Id.* at 114. The landlord began recording incoming calls on the advice of the police department because she had been receiving obscene telephone calls. *Id.* The landlord listened to the plaintiff's telephone call because she believed the caller made the obscene phone calls. *Id.* While listening to the conversation, the landlord began to suspect that the conversation concerned a drug transaction. *Id.* She notified the authorities and the plaintiff was arrested for drug trafficking. *Id.* The state superior court suppressed the recording on the ground that the plaintiff was unaware of the landlord's monitoring practice, and therefore did not consent. *Id.* The plaintiff contemporaneously filed his civil suit. *Id.*

81. *Id.* at 118. Presumably, the court based its conclusion on Griggs-Ryan's continued and unguarded telephone conversation. During the call which the landlord intercepted, Griggs-Ryan apparently spoke of a drug transaction. *Id.* at 114. He was arrested for drug trafficking because of the information the landlord overheard. *Id.*

determining implied consent, the court instead concluded that the scope of consent depends on the particular facts of each case.[82]

Both the First and Eleventh Circuit agree that the facts and circumstances of a case determine the extent of consent.[83] The two circuits differ, however, in their application of the concept of implied consent.[84] The *Griggs* court cited *Watkins* for the proposition that a court should not aggressively infer consent,[85] but also cited *Amen* for the rule that a court should interpret the consent requirement broadly.[86] Clearly, however, the character of notice given to the monitored party will largely determine whether a court chooses to infer consent.[87]

In addition to ambiguity surrounding the scope of the consent exception, courts have struggled with the applicability of the exception in cases involving restrictive state legislation. Under federal law, only one party to the conversation needs to consent to the interception for the exception to apply. Twelve states, however, require the consent of all the parties to the conversation in order to fall within the exception.[88] Both federal and

---

82. *Id.* at 119.

83. *Id.* at 117. The *Griggs* court reconciled its holding with *Watkins* by concluding that in each case, the existence or lack of consent is purely a factual question. *Id.*

84. *Id.* at 117. *Watkins*, 704 F.2d at 581.

85. 904 F.2d at 117. "[T]he ultimate determination must proceed in light of the prophylactic purpose of Title III—a purpose which suggests that consent should not casually be inferred." *Id.* (citing *Watkins*, 704 F.2d at 581).

86. *Id.* at 116-17 ("We agree with the Second Circuit that Congress intended the consent requirement to be construed broadly." (citing United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)).

87. *Compare* Griggs-Ryan v. Smith, 904 F.2d 112, 118 (1st Cir. 1990) ("Griggs-Ryan, of course, cannot plausibly posit a claim of deficient notice . . . [the landlord's] blanket admonishment left no room for plaintiff to wonder whether . . . the call would be intercepted.") *and* United States v. Amen, 831 F.2d at 378-79 (2d Cir. 1987) ("[Defendants] were on notice of the prison's interception policy from at least four sources . . . The two defendants had notice of the interception system and that their use of the telephones therefore constituted implied consent to the monitoring.") *with* Campiti v. Walonis, 611 F.2d 387, 393-94 (1st Cir. 1979) (refusing to imply consent where the inmates in a prison were not given notice that the calls could be monitored); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the capability of monitoring alone cannot be considered implied consent.") *and* Crooker v. United States Dept. of Justice, 497 F. Supp. 500, 503 (D. Conn. 1980) (prisoner's knowledge that calls were routinely monitored did not constitute consent to it).

88. California, CAL. PENAL CODE § 631(a) (West 1988); Connecticut, CONN. GEN. STAT. ANN. § 52-570(d)(a)(1) (West 1991); Delaware, DEL. CODE ANN. tit. 11, § 1335 (1975 & Supp. 1991); Florida, FLA. STAT. ANN. § 934.03(2)(d) (West 1991); Georgia, GA. CODE ANN. § 16-11-62(2) (Michie 1982); Kansas, KAN. STAT. ANN. § 21-4001 (1990); Maryland, MD. CTS. & JUD. PROC. CODE ANN. § 10-402(c)(3) (1990); Massachusetts, MASS. GEN. LAWS. ANN. ch. 272, § 99 (West 1991); Michigan, MICH. COMP. LAWS § 750.539c (1991); Oregon, OR. REV. STAT.

state courts have had great difficulty in determining whether state or federal law applies.[89] Moreover, an additional choice of law issue arises where a person places a telephone call between two states with conflicting consent exceptions.[90]

III. THE PROPOSED PRIVACY FOR CONSUMERS AND WORKERS ACT

In February 1991, sponsors of the proposed Privacy for Consumers and Workers Act ("Privacy Act") introduced the bill to Congress.[91] The

§ 165.540(1)(c) (1990); Pennsylvania, PA. STAT. ANN. tit. 18, § 5704(4) (1991); Washington, WASH. REV. CODE ANN. § 9.73.030(1)(a) (West 1988).

89. The only two district courts to confront the choice of law question in the context of civil cases reached opposite conclusions. In both cases, the federal one-party consent exception conflicted with a state statute requiring consent of every party.

In Montone v. Radio Shack, the court viewed the Pennsylvania wiretapping statute as a state evidentiary law because, under the statute, a victim of unlawful wiretapping may move to suppress the contents of the interception or the evidence derived from it. 698 F. Supp. 92, 94 (E.D. Pa. 1988). *See* PA. CONS. STAT. ANN. tit 18, § 5721 (1984). The court applied the federal rule and admitted the evidence. The court admitted it because, in a diversity case, the court must follow federal evidentiary law, unless one of the Federal Rules of Evidence specifically invokes state law. *Montone*, 698 F. Supp. at 93.

In contrast, in Navarra v. Bache Halsey Stuart Shields, Inc., the court held that the state had expressed a clear and unambiguous intent to provide additional protection for the privacy of its citizens, and therefore, no evidence obtained from wiretapping could be admitted without consent of all the parties. 510 F. Supp. 831, 836 (E.D. Mich. 1981).

State courts have also had difficulty determining the applicable law. In Hirschey v. Menlow, the Oregon Court of Appeals applied the one-party consent exception embodied in § 2511(2)(d) of Title III. 747 P.2d 402, 404 (Or. Ct. App. 1987). The court noted that § 2511(2)(d) also requires that the employer not intercept the communication "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state." *Id.* Concluding that a violation of the Oregon statute requiring consent of every party constituted a criminal or tortious act for the purpose of § 2511(2)(d), the court held that under Title III, the interception did not fall within the exception. *Id.* at 405.

In Jewelcor v. Pre-Fab Panelwall, Inc., the Pennsylvania Superior Court held that where conversations occur between people in different states, § 2511(2)(d) of Title III preempts state law. 579 A.2d 940 (Pa. Super. Ct. 1990).

90. In United States v. Nelson, the Eleventh Circuit held that the definition of "the term 'intercept' as it relates to 'aural acquisition' refers to the place in which the communication is obtained regardless of where the communication is ultimately heard." 837 F.2d 1519, 1527 (11th Cir. 1988). Therefore, under *Nelson*, the location of the intercept determines the applicable law. However, the definition of "intercept" under state law is not always identical to the definition of "intercept" under Title III. *See* Munroe, *supra* note 4, at 12.

91. Representative Pat Williams of Montana introduced the bill to the House of Representatives on February 28, 1991. 137 CONG. REC. H1325 (1991). Currently, the bill has a total of 131 co-sponsors: 119 Democrats and 12 Republicans. 137 CONG. REC. H11891 (1991).

Senator Paul Simon of Illinois introduced the bill to the Senate on February 27, 1991. 137 CONG. REC. S2404 (1991). To date, the bill has one co-sponsor in the Senate. 137 CONG. REC. S4063 (1991).

purpose of the bill is to "prevent potential abuses of electronic monitoring in the workplace."[92] Under the Privacy Act, "electronic monitoring" encompasses all data collection by any technological device, excluding only wiretapping and the electronic transfer of payroll information.[93] The proposed legislation regulates any individual, business entity, or governmental body which has employees.[94] If enacted, the legislation will severely impact employers who engage in electronic monitoring by establishing specific guidelines for legal monitoring.

Under the proposed Act, an employer must comply with five requirements before instituting or maintaining an electronic monitoring system. First, a monitoring employer must post a notice of electronic monitoring on its premises in a conspicuous place.[95] Second, the employer must provide specific information to each monitored employee including the type of monitoring device, the type of data collected, the frequency with which monitoring will occur, and how the employer will use the data to evaluate performance.[96] However, the employer does not have to pro-

---

92. H.R. 1218, *supra* note 20.

93. Section 2(1) provides:

(1) ELECTRONIC MONITORING. —

(A) IN GENERAL. — Except as provided in subparagraph (C), the term "electronic monitoring" means the collection, storage, analysis, or reporting of information concerning an employee's activities by means of a computer, electronic observation and supervision, telephone service observation, telephone call accounting, or other form of visual, auditory, or computer-based technology which is conducted by any method other than direct observation by another person, including the following methods: Transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature which are transmitted in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system. . . .

(C) EXCLUSION. — The term "electronic monitoring" does not include—

(i) wiretapping, or

(ii) the electronic transfer of payroll and other payroll-related information for payroll purposes only.

H.R. 1218, *supra* note 20, § 2(1)(A).

94. H.R. 1218, *supra* note 20, § 2(3).

95. Section 3(a)(1) provides:

(a) IN GENERAL. —

(1) FIRST NOTICE. — The Secretary [of Labor] shall prepare, have printed, and distribute to employers a notice which will inform employees—

(A) that an employer engages in or may engage in electronic monitoring of employees and specifies the circumstances (including monitoring described in paragraph (3)) under which an employee is or is not entitled to additional notice under this section, and

(B) of the rights and protections provided to employees by this Act.

[With the exception of the 90 days immediately following enactment], each employer who engages in electronic monitoring shall post and maintain such notice in conspicuous places on its premises where notices to employees are customarily posted.

H.R. 1218, *supra* note 20, § 3(a)(1).

96. Section 3(a)(2) provides in pertinent part:

(2) SPECIFIC NOTICE. . . . [I]f an employer proposes to engage in electronic monitoring

vide specific notice where the employer has a reasonable suspicion that an employee is engaging in criminal conduct which will adversely affect the employer's interests.[97] Third, the employer must notify prospective employees of the monitoring practice at the job applicant's initial interview.[98] Fourth, an employer who only periodically monitors conversations must install a device which alerts employees each time the employer monitors.[99] Similarly, where an employer continuously monitors employees, but only sporadically reviews the data during the monitoring, the employer must alert employees each time it reviews the data.[100] Finally, an employer who tests the quality of customer service

---

of an employee, the employer shall provide such employee with prior written notice describing the following regarding the electronic monitoring of the employee:

(A) The forms of electronic monitoring to be used.

(B) The personal data to be collected.

(C) The frequency of each form of electronic monitoring which will occur.

(D) The use to be made of personal data collected.

(E) Interpretation of printouts of statistics or other records of information collected through electronic monitoring.

(F) Existing production standards and work performance expectations.

(G) Methods for determining production standards and work performance expectations based on electronic monitoring statistics.

H.R. 1218, *supra* note 20, § 3(a)(2).

97. Section 3(a)(3) provides:

(3) EXCEPTIONS TO NOTICE REQUIREMENT.—

(A) SPECIAL MONITORING.— If an employer has a reasonable suspicion that an employee is engaged in conduct which

(i) violates criminal or civil law, and

(ii) adversely affects the employer's interests or the interests of such employer's employees, and if the employer engages in electronic monitoring of such conduct, the employer is not required to provide the employee with the notice prescribed by paragraph (2).

H.R. 1218, *supra* note 20, § 3(a)(3).

98. Section 3(a)(4) provides:

(4) NOTICE TO PROSPECTIVE EMPLOYEES.—

(A) IN GENERAL.— Each employer shall notify a prospective employee at the first personal interview of existing forms of electronic monitoring conducted by the employer which may affect the prospective employee if such employee is hired by the employer.

(B) SPECIFIC NOTICE.— Each employer, upon request by a prospective employee or when the employer offers employment to a prospective employee, shall provide the prospective employee with the written notice described in [§ 3(2)] regarding existing forms of electronic monitoring conducted by the employer which may affect the prospective employee is such employee is hired by the employer.

H.R. 1218, *supra* note 20, § 3(a)(4).

99. Section 3(a)(5) provides in pertinent part:

(5) NOTICE OF PERIODIC OR RANDOM MONITORING. . . . [A]ny employer who conducts electronic monitoring of an employee on a periodic or random basis shall provide the employee with a simultaneous notice in the form of a signal light, beeping tone, verbal notification, or other form of visual or aural notice that indicates electronic monitoring is being conducted.

H.R. 1218, *supra* note 20, § 3(a)(5).

100. Section 3(a)(6) provides in pertinent part:

by monitoring employee telephone calls must use a device which notifies the customer that the employer is listening to the conversation.[101]

Additional provisions of the proposed legislation severely restrict the employer's ability to utilize information obtained through electronic monitoring. Under the Act, an employer may not evaluate work performance or set production goals or quotas solely on the basis of information acquired by monitoring employee actions.[102] Moreover, not only does the Act strictly limit the type of information an employer may collect through electronic monitoring, but it also regulates the employer's disclosure of this information.[103] The Act also contains other require-

---

(6) NOTICE OF REVIEW OF CONTINUOUS ELECTRONIC MONITORING.—
(A) REVIEW DURING MONITORING.—
(i) IN GENERAL.— Except as provided in . . . clause (ii), any employer who reviews data, obtained by continuous electronic monitoring of the employer's employees, on a periodic or random basis while the monitoring is being conducted shall provide the employee with a simultaneous notice in the form of a signal light, beeping tone, verbal notification, or other form of visual or aural notice that indicates the electronic monitoring is being reviewed.
(ii) The review of electronic data obtained from the use of an electronic card access system and the review of data appearing simultaneously on multiple television screens are not subject to clause (i).
(B) REVIEW AFTER MONITORING.— An employer may review data obtained by continuous electronic monitoring of the employer's employees after the monitoring was completed only if review was limited to specific data which the employer has reason to believe contains information relevant to an employee's work.

H.R. 1218, *supra* note 20, § 3(a)(6).

101. Section 3(b) provides in pertinent part:

(b) CUSTOMER NOTICE.— . . . [I]f an employer engages in telephone service observation, the employer shall provide the customer who is [the] subject of the observation with a simultaneous notice in the form of a signal light, beeping tone, verbal notification, or other form of visual or aural notice, at periodic intervals, indicating that telephone service observation is taking place.

H.R. 1218, *supra* note 20, § 3(b).

102. Section 6(b) provides:

(b) DATA SHALL NOT BE USED AS SOLE BASIS FOR EVALUATION OR PRODUCTION QUOTAS.—An employer shall not use personal data obtained by electronic monitoring as—
(1) the sole basis for individual employee performance evaluation, or
(2) the sole basis for setting production quotas or work performance expectations.

H.R. 1218, *supra* note 20, § 6(b).

103. Under § 5 of the Act, an employer may only intentionally collect information related to an employee's work performance. However, the Act does not prohibit inadvertent monitoring of information unrelated to an employee's work performance or the collection of data unrelated to an employee's work performance. H.R. 1218, *supra* note 20, § 5(a).

An employer may only disclose information obtained by monitoring to: (1) the affected employee; (2) officers and supervisors who have a legitimate need for the information; (3) law enforcement agencies in conjunction with a criminal matter; or (4) pursuant to a court order. H.R. 1218, *supra* note 20, § 5(b)(1).

The employer may disclose information if it contains evidence of illegal conduct by a public offi-

ments which further protect the employee's interests.[104]

The proposed Act and Title III provide similar remedies to an employee. Any employee affected by a violation of the Act may bring a private civil action against the employer for appropriate relief including reinstatement, promotion, lost wages and benefits.[105] Additionally, the Secretary of Labor may initiate an action to enjoin violations of the Act or assess a civil penalty of $10,000 per violation.[106]

IV. A CRITIQUE OF THE TITLE III EXCEPTIONS AND THE PROPOSED PRIVACY FOR CONSUMERS AND WORKERS ACT

Title III of the Omnibus Crime Control and Safe Streets Act only indirectly governs employee monitoring through its total ban on the interception of wire, oral and electronic communications.[107] Congress did not design Title III to regulate the conduct of employers, but rather intended the legislation to balance the privacy expectations of the individual against the legitimate needs of law enforcement agencies.[108] Consequently, Title III fails to address the discrete problem of electronic monitoring in the work place.[109]

---

cial or if nondisclosure would result in "a direct and substantial effect on public health or safety." However, the employer must notify the employee before proceeding with the disclosure. If the employee objects, the employer must obtain a court's permission before disclosing the information. H.R. 1218, *supra* note 20, § 5(b)(2).

104. For example, § 4 requires an employer to provide an employee with the opportunity to review all personal data gathered by electronic means. Section 5(c) prohibits an employer from monitoring restrooms, locker rooms or dressing rooms in the absence of suspected criminal activity. Section 6(a) restrains an employer from taking any action against an employee, unless the employer has satisfied the provisions of the Act regarding notice and the type of the information collected. H.R. 1218, *supra* note 20, § 6(a).

105. Section 7(c) provides in pertinent part:

> (c) PRIVATE CIVIL ACTIONS.—
>
> (1) IN GENERAL.— An employer who violates this Act shall be liable to the employee or prospective employee affected by such violation. Such employer shall be liable for such legal or equitable relief as may be appropriate, including employment, reinstatement, promotion, and the payment of lost wages and benefits.

H.R. 1218, *supra* note 20, § 7(c).

Section 8 of the Act prohibits an employer from taking any retaliatory action against an employee who brings a private civil action pursuant to § 7(c). H.R. 1218, *supra* note 20, § 8.

106. H.R. 1218, *supra* note 20, § 7(a).

107. Prior to 1986, Title III protected wire and oral communications, but did not regulate the use of electronic or computerized monitoring. In 1986, Congress amended Title III to cover all electronic communications, thus bringing computerized monitoring within its protection. *See supra* notes 28-31 and accompanying text.

108. *1986 Senate Report*, *supra* note 30, at 3559.

109. Current law does not provide an effective balance between employer and employee rights.

A. *Ineffective Regulation of Work Place Electronic Monitoring under Title III*

Under Title III, Congress provided two narrow exceptions to the general prohibition against electronic surveillance: the consent exception and the business-extension exception.[110] Even though an employer must fall within one of these exceptions to legally intercept any electronic communication, government officials estimate that the nation's employers monitor approximately six million workers.[111]

Although Title III affords litigants a private right of action against an employer who unlawfully intercepts employee communications, employees have rarely challenged their employer's monitoring practices in court.[112] Attempting to explain this phenomenon, the Office of Technology Assessment has suggested that the inadequacy of current legal remedies explains the paucity of lawsuits.[113]

For example, the business-extension exception fails to effectively regulate the relationship between employers and employees. Specifically, unresolved ambiguities regarding the coverage of the exception expose the employer to significant and unforeseen legal liability, and also hinder the employee's ability to bring a successful civil action.[114] Because it is difficult to predict how a court will interpret the extent of the exception, employers who engage in electronic monitoring expose themselves to substantial liability. Employees who institute civil lawsuits may fail to recover because of a court's misguided reading of the exception.[115]

See Hearings on H.R. 1218, *supra* note 18, at 74 (testimony of Lewis Maltby, Director, ACLU National Task Force on Workplace Rights, and Janlori Goldman, Director, ACLU Project on Privacy and Technology) ("Employers need information about job performance, but that need must be balanced against employees' reasonable expectations of privacy. Unfortunately, current law does not strike such a balance. In fact, it does not even attempt to strike a balance.").

110. *See supra* notes 8-9 and accompanying text. *See also*, *OTA Report*, *supra* note 1, at 109.

111. *See OTA Report*, *supra* note 1, at 5.

112. *Id.* at 22.

113. The small number of lawsuits also supports the conclusion that Congress cannot assess the type of legal inadequacies in the current law until the judiciary acts. *Id.* This conclusion, however, clearly illustrates the need for swift congressional action. If employers monitor 6,000,000 workers, but few employees pursue legal remedies because of the inadequacy of the existing law, the judiciary will not have the opportunity to act because few cases will come before the courts. If Congress stalls and waits for the judiciary to act, an eternal holding pattern will likely result.

114. *See* Munroe, *supra* note 4, at 11.

115. *See supra* notes 12-14 and accompanying text. Employers found liable in an action under Title III are subject to substantial monetary penalties. In 1986, Congress amended the provisions of Title III governing criminal sanctions and civil damages. Currently, the maximum statutory criminal penalty is $250,000 for individuals and $500,000 for organizations. In addition, Congress in-

In particular, the rapid rate of technological advancement has rendered the business-extension exception largely inapplicable. When Congress amended Title III in 1986 to encompass all electronic communications, Congress did not amend the language of the business-extension exception.[116] By definition, the business-extension exception only provides a safe harbor to employers where a telephone or telegraph instrument is the device used to intercept the communication.[117] The amendments enacted in 1986 failed to address whether the exception will provide a safe harbor when an employer utilizes an electronic monitoring device as the intercepting device.[118] Therefore, communications intercepted through the use of a computer program may fall outside the business-extension exception because Congress did not include a computer program in the statute's definition of a telephone or telegraph instrument.[119]

Nevertheless, many employers engage in covert, nonconsensual monitoring by the use of computerized equipment, such as advanced computer software.[120] For example, a new software package called "Peek

---

creased civil statutory damages to $10,000 per violation. *See also* Burnside, *supra* note 31, at 509 (citing 18 U.S.C. § 3571(b) (Supp. 1985) and 18 U.S.C.A. § 2520 (c)(2)(B) (West Supp. 1987)).

116. *See* 18 U.S.C. § 2510(5)(a) (1988). Prior to the 1986 amendments, Title III did not encompass communications between machines and computers. *See* Burnside, *supra* note 31, at 482-83. Consequently, before 1986, Title III protected communication between two people, but did not address the same communication when transmitted between a person and a machine or between two machines. *Id.* For a discussion of the specific types of equipment encompassed by Title III following the 1986 amendments, see *supra* note 31 and accompanying text.

117. 18 U.S.C. § 2510(5)(a) (1988).

118. The legislative history of the 1986 amendments does not provide any guidance as to whether Congress intended the business-extension exception only to cover telephone or telegraph equipment. Congressional oversight may explain the failure to amend the exception.

119. Prior to the 1986 amendments, legislators generally conceded that the definition of "wire communication" did not encompass computer technology. *See* S. REP. No. 541, 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 ("[T]here are no comparable Federal statutory standards to protect . . . new forms of telecommunications and computer technology."). If the broader definition of "wire communication" failed to encompass computer technology, the narrower requirement of the business-extension exception, relating to the nature of the intercepting device, clearly does not encompass computerized intercepting devices. The statute provides no guidance as to whether the "telephone or telegraph component" requirement would encompass a device that contained a telephone or telegraph component, such as an internal modem. *Cf.* Abel v. Bonfanti, 625 F. Supp. 263, 270 (S.D.N.Y. 1985) (holding that as long as an intercepting device is attached to an extension telephone outlet, the business-extension exception will apply).

120. Laura M. Litvan, *Unions Fight Hightech Job Monitoring*, WASH. TIMES, Feb. 16, 1990, at C1. *See also Hearings on H.R. 1218*, *supra* note 18, at 2 (statement of Rep. Pat Williams, Chairman) ("According to the May 13, 1991 issue of 'Info World,' there are currently 11 such [monitoring] programs in existence.").

and Spy" allows a supervisor to monitor the data appearing on an employee's computer screen at any moment in time.[121] Courts have not yet addressed the legality of such practices under the Title III exceptions. However, the 1986 amendments to Title III clearly protect computer-to-computer, or computer-to-individual, electronic communications.[122] Thus, Title III technically prohibits these computerized monitoring programs.

Even when the business-extension exception applies, courts differ in determining whether the interception of personal telephone calls is encompassed within the "ordinary course of business." In *Watkins v. L.M. Berry Co.*,[123] the Eleventh Circuit held that the interception of business calls conclusively falls within the ordinary course of business, but the exception does not apply to the monitoring of personal calls.[124] The *Watkins* court defined a business call as a conversation in which the employer had a legal interest.[125] However, only three years later, in *Epps v. St. Mary's Hospital of Athens, Inc.*,[126] the same court severely manipulated the *Watkins* court's definition of a business telephone call to include a personal telephone call in the protected business call category.[127]

---

121. Litvan, *supra* note 120, at C1. Other examples of computer monitoring devices include: a trucking firm that uses computer technology to time drivers' rest stops, or software that permits a supervisor to view an employee's daily appointment schedule without alerting that employee. *Id.*

122. *1986 Senate Report*, *supra* note 30, at 3568. The legislative history states: "As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice. Communications consisting solely of data, for example . . . are electronic communications." *Id.*

123. 704 F.2d 577 (11th Cir. 1983).

124. *Id.* at 583. The *Watkins* court specifically held that an employer may not intercept a personal call in the ordinary course of business, except to the extent necessary to determine unauthorized use of the telephone. *Id.*

125. *Id.* at 582.

126. 802 F.2d 412 (11th Cir. 1986), *reh'g denied*, 867 F.2d 999 (11th Cir. 1986).

127. In *Watkins*, a supervisor intercepted a call in which the employee discussed alternative employment possibilities. 704 F.2d at 579. The court held that the employer had no legal interest in a telephone call in which an employee discussed alternative employment possibilities because the employee was free to resign at will. *Id.* at 582. *See supra* notes 50-51 and accompanying text. The court concluded that the employer violated Title III when it intercepted a personal telephone call. 704 F.2d at 582.

Yet, in *Epps*, the Eleventh Circuit, professing to apply the legal interest test, concluded that a telephone conversation between two employees in which they gossiped about supervisors constituted a business call. 802 F.2d at 417. The court based this finding on the fact that the call occurred during business hours, between employees, over a hospital extension and concerned supervisory employees. *Id.*

However, virtually the same facts were present in *Watkins* where the Eleventh Circuit held that the conversation was a personal call. In *Watkins*, not only did the employee make the call during

While the holding of *Watkins* may appear definitive on the issue of classifying a call within the ordinary course of business exception, no intelligible standard exists for determining whether a particular conversation constitutes a personal or business call.[128]

Finally, courts have also inconsistently answered the question of whether surreptitious monitoring is ever encompassed within the scope of the "ordinary course of business" requirement. The Tenth Circuit, in *United States v. Harpel*,[129] specifically held that to protect surreptitious monitoring within the business-extension exception would violate the purpose of Title III.[130] However, the Fifth Circuit, in *Briggs v. American Air Filter, Inc.*,[131] held that the ordinary course of business exception includes surreptitious monitoring if the employer limits the monitoring in purpose and time.[132] Some commentators suggest that Congress never intended the business-extension exception to protect surreptitious monitoring if conducted through an extension telephone.[133]

The consent exception is equally ineffective in regulating the employer-

---

business hours, but it concerned the employee's continued employment. The court did not explain how an employer has a greater legal interest in the gossip of an employee than the same employer would have in the continued employment of the employee.

128. *See* Munroe, *supra* note 4, at 13. Munroe argued that *Epps* provided employers with some indication of what constitutes a personal call, but employers should not interpret the case as an automatic authorization to monitor employee gossip. *Id.* at 14. Munroe suggested that employers adopt a blanket policy of not monitoring personal calls, rather than forcing a supervisor to make a split-second decision on whether the employer has a legal interest in monitoring the call. *Id.*

129. 493 F.2d 346 (10th Cir. 1974).

130. In *Harpel*, the court held that surreptitious monitoring violated the privacy interests of the individual which Congress intended to protect in enacting Title III. *Id.* at 351-52. *See* Burnside, *supra* note 31, at 487 n.239.

In Campiti v. Walonis, the First Circuit also questioned the propriety of applying the business-extension exception to cases involving covert monitoring. 611 F.2d 387 (1st Cir. 1979). The *Campiti* court noted that the legislative history of Title III indicates that Congress intended to prohibit all surreptitious monitoring. 611 F.2d at 392 n.5. The court relied on the Title III Senate Report which declared a complete ban on unauthorized electronic surveillance except for surveillance conducted by authorized law enforcement officers. *Id.* (citing S. REP. NO. 1097, 90th Cong., 2d Sess. (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2113).

131. 630 F.2d 414 (5th Cir. 1980).

132. *Id.* at 420. *See supra* notes 41-45 and accompanying text.

133. *See* Burnside, *supra* note 31, at 488 (citing Bruce E. Fein, *Regulating the Interception and Disclosure of Wire, Radio and Oral Communication: A Case Study of Federal Statutory Antiquation*, 22 HARV. J. ON LEGIS. 47, 92 (1985)). Burnside suggested that Congress intended the business-extension exception to prevent the imposition of liability on an employer who inadvertently intercepted a conversation through use of the equipment in the ordinary course of business. *Id.* at 488.

Yet, if Congress intended the business-extension exception to merely protect inadvertent interceptions through extension telephones, then the types of interceptions in *Watkins*, *Briggs* and *Epps*

employee relationship. Given the uncertainty regarding the scope of the business-extension exception, many employers attempt to limit their legal exposure by requiring an employee to consent to the monitoring before accepting employment.[134] However, the employer may condition continued employment on the employees' acceptance of an onerous or intrusive monitoring policy.[135]

Not only is the "prior consent" exception ineffective in protecting employee interests, but it also fails to safeguard employers from unwarranted exposure to Title III civil liability. Title III only protects an employer from liability if the employee expressly or impliedly consents to the monitoring.[136] In *Watkins v. L.M. Berry Co.*,[137] the Eleventh Circuit limited the scope of express consent by holding that consent is not an all-or-nothing proposition.[138] The *Watkins* court also held that a jury must determine if the employee's consent encompassed the particular monitored call at issue.[139] In the context of implied consent, courts routinely evaluate the scope of consent based on the facts of each individual case.[140] Consequently, an employer cannot effectively predict its expo-

---

would clearly fall outside the exception. In all three cases, the employer wilfully, rather than inadvertently, intercepted the call. *See supra* notes 123-32 and accompanying text.

Burnside also argued that interpreting the business-extension exception to protect only accidental interceptions is consistent with the Title III prohibition on willful interceptions. Burnside, *supra* note 31, at 488 n.249. However, Burnside's interpretation would read the business-extension exception out of the statute. Title III only prohibits intentional interceptions. *See* 18 U.S.C. § 2511 (1988). Hence, an exception protecting inadvertent interceptions is useless.

134. Furfaro & Josephson, *supra* note 3, at 3.

135. Monitoring in the workplace raises a variety of concerns including privacy, stress and health, worker dignity and quality of work environment. *OTA Report*, *supra* note 1, at 186-87. A field study revealed that fairness is critical to employee acceptance of a monitoring program. *Id.* at 187 (citing Alan Westin & The Educational Fund for Individual Rights, *Privacy and Quality of Work Life Issues in Employee Monitoring*, contractor paper prepared for OTA, May 1986 (field study conducted during 1982-84, and updated at all 110 sites during 1985-86). If an employer can offer continued employment to gain employee consent, then the employer does not have to institute a fair or just monitoring policy.

136. *See* Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) ("[W]e—and other courts—have held that Title III affords safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent.").

137. 704 F.2d 577 (11th Cir. 1983).

138. *Id.* at 582.

139. *Id.* The *Watkins* court stated that the fact finder must decide the scope of the employee's consent and then determine "whether and to what extent the interception exceeded that consent." *Id.*

140. *See, e.g.*, Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990) ("The circumstances relevant to an implication of consent will vary from case to case."); United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987), *cert. denied*, 485 U.S. 1021 (1988) (implying consent from the surrounding

sure to Title III liability.

In order to avoid a fact-specific inquiry, a prudent employer must obtain the employee's express, written consent to monitor every telephone call placed by the employee regardless of the nature of the conversation.[141] As a result, an employer is precluded from implementing a monitoring policy which meets the employer's specific objectives for monitoring while minimizing the intrusion on the employees' privacy. Judicial interpretations of the consent exception force employers to adopt continuous or constant monitoring policies.[142] However, constant monitoring detrimentally impacts the work environment because it poses a more serious threat to the employee's mental health than periodic monitoring.[143]

Yet, an employer cannot completely avoid liability by obtaining express consent to monitor every employee phone call.[144] Twelve states require that every party in the conversation consent to the monitoring.[145] Courts have struggled with choice of law questions concerning the application of federal or state law, and the proper state law to apply in interstate controversies.[146] For example, regional or national companies may engage in conduct that one state permits but another state prohibits.[147]

B. The Proposed Privacy for Consumers and Workers Act: Unsuitable Interference with the Employer's Autonomy

The proposed Privacy for Consumers and Workers Act adequately

---

circumstances which showed that the prisoners knowingly agreed to the prison official's surveillance).

141. Munroe, *supra* note 4, at 12. Munroe noted that *Watkins* demonstrates that a court will evaluate each interception separately to determine whether the interception fell within the employer's announced monitoring policy. *Id.* Yet, compliance with Title III does not ensure that a court will not hold an employer liable under a more stringent state wiretapping law. *See supra* notes 88-90 and accompanying text.

142. *See supra* note 141 and accompanying text.

143. *OTA Report, supra* note 1, at 96. The OTA Report recognized that the frequency of monitoring is an important criterion in evaluating its effects because, in addition to "continuousness" and "regularity," an employer's frequency distinguishes spot-check monitoring for efficiency and a constantly monitored work environment. *Id.*

144. *See* Munroe *supra* note 4, at 12 (explaining that because of inconsistencies with state legislation, a company engaged in telemarketing cannot feel relieved merely because it complied with Title III requirements).

145. *See supra* note 88 and accompanying text.

146. *See supra* notes 89-90 and accompanying text.

147. *See* Munroe, *supra* note 4, at 12. Overlapping state statutes and Title III provisions further complicate the ambiguities surrounding the two exceptions. *Id.*

protects the privacy of the employee at the expense of the autonomy of the employer.[148] First, the requirement that employers notify employees by a beep or flashing light unduly burdens the employer's ability to provide cost-effective customer service. [149] This requirement will prohibit the employer from accurately assessing employee performance.[150] In addition, any method of providing notice, whether by a beeping sound or flashing light, will distract the employee from his duties long enough to increase costs and decrease the quality of customer service.[151] Moreover,

148. The proposed Act protects the employee's privacy interest by requiring the employer to issue specific notice of the form of monitoring used, the type of data collected and the method the employer will use the data in evaluating performance. H.R. 1218, *supra* note 20, § 3(a)(2). The proposed Act requires employers to notify prospective employees of the monitoring policy. *See supra* note 98. Additional protections for the employee include: a private right of action against employers who violate the Act; a complete prohibition on monitoring in private areas, such as bathrooms, locker rooms; and, a "whistleblower" provision to prevent an employer from disciplining or discharging an employee for bringing an action under the Act. *See supra* note 96. *See also supra* notes 104-05 and accompanying text.

149. H.R. 1218, *supra* note 20, § 3(a)(5)-(6) (1991). *See generally supra* note 99 and accompanying text.

150. *See Hearings on H.R. 1218*, *supra* note 18, at 59 (statement of Richard A. Barton, Senior Vice President of Government Affairs, The Direct Marketing Association). "Signal lights, beep tones or other visual or sound notices would hinder the purposes behind telephone monitoring. The simple fact that an employee knows he or she is being monitored may change the behavior of the employee and make it impossible to gain an accurate reading of that employee's performance." *Id.*

Thomas M. Flood, Vice President and General Manager for Operator Services at Pacific Bell, recognized that: "Monitoring with notice only tends to destroy the objectivity of the supervisory monitoring sample and render monitoring, as a tool for measuring the overall service provided to the customer, of little value. Monitoring with notice precludes management from discovering and correcting unsatisfactory employee performance." *Id.* at 113 (statement of Thomas M. Flood).

In a written statement, the United States Telephone Association stated: "Some employees would modify their behavior on calls when they knew they were being observed, thus spoiling the spontaneity that observing offers to management to determine how customers are being treated." *Id.* at 214 (statement of the United States Telephone Association).

151. The Direct Marketing Association contended that beep tones will likely distract and confuse both employees and customers. The Association argued that aural or visual forms of notice will jeopardize the employee's ability to perform his job accurately, thus increasing errors in customer accounts. *Id.* at 59 (statement of Richard A. Barton, Senior Vice President, Government Affairs, The Direct Marketing Association).

Thomas M. Flood, Vice President and General Manager for Operator Services at Pacific Bell, stated that providing an individual employee notice that the employer is monitoring him, instead of giving all employees a group notice that the employer is monitoring, may actually decrease the level and quality customer service. *Id.* at 113 (statement of Thomas M. Flood).

The Air Transport Association of America stated that aural methods of notification will disrupt airline telephone reservation systems by requiring the employee to explain to the customer why the line is beeping. As a result, airlines will have to hire either additional reservation agents or force customers to wait longer to speak with an agent. The Association argued that either result would increase consumer costs. *Id.* at 197 (statement of Air Transport Association of America).

knowledge of the specific instances of monitoring may adversely affect the employee's state-of-mind rather than effectively protect the employee's privacy.[152] The simultaneous notice requirement unnecessarily interferes with the employer's business.

Second, the proposed Act defines "electronic monitoring" too broadly.[153] The scope of "electronic monitoring" protected by the Act encompasses many employer security measures such as card access systems, security camera surveillance, inventory control systems and cash registers.[154] All of these devices collect data intentionally and indiscriminately.[155] However, the Act only permits employers to intentionally collect data about an employee that relates to that employee's work.[156] The Act does not define the scope of an "employee's work" in relation to this

152. *Id.* at 59 (statement of Richard A. Barton, Senior Vice President, Government Affairs, Direct Marketing Association). Barton argued that knowledge of monitoring may not only change the behavior of an employee, but also may increase stress. The employee's performance may deteriorate because of the higher stress level induced by knowledge of the monitoring. Barton noted that because of the increase in stress level, many telemarketing employees prefer that the employers notify them when the employer monitors employees. *Id.*

153. H.R. 1218, *supra* note 20, § 2(a)(A).

154. Section 2(1)(A) of the Act defines "electronic monitoring" to include: "the collection, storage, analysis, or reporting of information . . . by means of a computer, electronic observation and supervision . . . or other form of visual auditory, or computer-based technology which is conducted by any method other than direct observation." *See supra* note 93. Many employers that appeared before the Subcommittee on Labor-Management Relations assumed that this definition encompassed security devices. *See Hearings on H.R. 1218*, *supra* note 18, at 78-79 (statement of Vincent L. Ruffolo, President of A & R Securities) (noting in his testimony that the definition of "electronic monitoring" would encompass card access systems, security camera surveillance and reviews of bank and telephone credit card usage); *id.* at 202 (statement of the National Retail Federation) (contending that H.R. 1218's scope exceeds telephone monitoring and apparently encompasses monitoring and collecting information through every and all imaginable types of electronic equipment or devices including computers, cash registers, video machinery, calculators and inventory control equipment).

155. The proposed Act does exempt an employer who inadvertently collects data which is not confined to an employee's work. H.R. 1218, *supra* note 20, § 5(a)(2); *see generally supra* note 103 (no liability for inadvertent collection of data). However, the Act fails to define what constitutes an inadvertent interception of information that is not related to an employee's work. For example, a court could construe an inadvertent interception narrowly to include accidental interceptions of information which are not work related. Alternatively, a court could interpret an inadvertent interception of data unrelated to an employee's work to encompass all personal data collected by general surveillance mechanisms. Under the broader definition, however, the requirement that employers confine all personal data to an employee's work loses all force. Yet, only the broader construction of an "inadvertent exception" would allow general surveillance cameras to avoid the requirement that gathered data relate to the employee's work. The exception will eventually envelop the rule.

156. Section 5(a)(1) prohibits an employer from intentionally collecting personal data about an employee that is not confined to the employee's work. H.R. 1218, *supra* note 20, § 5(a)(1); *see generally supra* note 103. The Act defines "personal data" as "any information concerning an employee which, because of name, identifying number, mark, or description, can be readily associated

requirement. Consequently, the statute may not permit security camera surveillance because it falls within the protected "electronic monitoring" category, and the information collected may not fall within the statute's definition of "employee's work."[157] Thus, the proposed Act would disrupt the employer's ability to provide security measures, which prevent loss and ensure customer and employee safety.[158]

Finally, the Act unnecesarily limits the employer's ability to assess information obtained through electronic monitoring. Under the proposed Act, an employer may not use data collected by electronic monitoring as the sole basis for evaluating employees or setting production expectations.[159] This provision severely inhibits the employer's right to decide which individuals to employ or promote.[160] If all of the employee's work performance occurs on the telephone or the computer, the statute leaves the employer with only a small amount of reliable information on which

---

with a particular individual, and such term includes information contained in printouts, forms, or written analyses or evaluations." H.R. 1218, *supra* note 20, § 2(4).

157. Clearly, an individual's picture on a videotape would fall within the somewhat vague definition of "personal data." *See supra* note 156. However, a security camera records everything within the scope of its lens, not just information related to a particular individual's work performance. *See Hearings on H.R. 1218*, *supra* note 18, at 81 (statement of Vincent L. Ruffolo, President of A & R Securities) "Businesses where security camera surveillance is in place cannot distinguish, for observation and recording purposes, between work performance-related and other activities of employees." *Id.*

158. *Hearings on H.R. 1218*, *supra* note 18, at 204 (statement of the National Retail Federation) ("A comprehensive survey . . . demonstrates the value of commonly used loss prevention equipment and systems that would fall under the bill's extremely wide-ranging definition of 'electronic monitoring' . . . Mass retailers employ these and similar devices for numerous legitimate reasons: to counter the serious problems of internal and external theft and to assure the safety of their customers and employees." *Id.*

159. H.R. 1218, *supra* note 20, §§ 6(b)(1), 6(b)(2). *See also supra* note 102 and accompanying text.

The purpose of the restriction on setting production quotas or work performance expectations is unclear. Moreover, the bill fails to specify whether the prohibition applies solely to data collected on one individual or to aggregate data of a particular group. This data may constitute the most logical source of information regarding acceptable production goals or quotas. *See Hearings on H.R. 1218*, *supra* note 18, at 199 (statement of the Air Transport Association of America) ("There is nothing inherently wrong in using electronic monitoring for that purpose.").

160. *See Hearings on H.R. 1218*, *supra* note 18, at 114 (statement of Thomas M. Flood, Vice President and General Manager for Operator Services at Pacific Bell) ("The legislation should consider an employer's right to take appropriate action under extreme circumstances."); *see id.* at 182-83 (statement of The Food Marketing Institute) ("A restriction of this kind would severely limit an employer's ability to evaluate the job performance of certain employees, such as truck drivers, data processors, claims adjusters and other individuals who work with point-of-sale equipment and computers.").

to base an employment decision.[161] Furthermore, the provision prevents an employer, who discovers that an employee is involved in illegal activity or theft, from taking disciplinary action based solely on the electronically acquired information.[162] Employers should retain full discretion in establishing criteria for both hiring employees and their continued employment.

V. A PROPOSAL FOR FEDERAL REGULATION OF ELECTRONIC MONITORING IN THE WORKPLACE

Congress should approach the problem of monitoring in the work place from a different perspective. Both Title III and the Privacy for Consumers and Workers Act focus on specific methods of monitoring and specific monitoring equipment.[163] This approach fails to remedy the problem for two reasons. First, the law cannot immediately adapt to changes in technology.[164] Second, the problems with the proposed Act

161. *See Hearings on H.R. 1218*, *supra* note 18, at 183 (statement of the Food Marketing Institute) ("Because of the increasing size of the workforce and the changing nature of many jobs the only effective way to evaluate some employees may be by electronic means with analysis or review of collected data and print-outs. Under section 6(a), how does an employer evaluate a worker who has a computer at home? . . . Electronic data may be the only *objective* measure of employee performance.").

162. *See Hearings on H.R. 1218*, *supra* note 18, at 205 (statement of the International Mass Retail Association, Inc.) ("Would the interests of the company, its customers or fellow workers be better served by allowing the dishonest or unsatisfactory worker to remain in place until the same conduct is repeated, this time before an eyewitness?"); *see id.* at 183 (statement of the Food Marketing Institute) ("In our opinion, the language contained in section 6(a) is extremely broad and will likely prevent or delay an employer from taking appropriate action, such as disciplining or firing an employee who is observed through electronic monitoring to have stolen merchandise, money from a cash register or controlled drugs from the pharmacy department.").

163. For example, Title III defines "electronic monitoring" in terms of the specific equipment covered by the Act. Title III includes information transferred by "wire, radio, electromagnetic, photoelectronic or photooptical system[s]" but excludes cordless telephones, tone-only paging devices and tracking devices. 18 U.S.C. § 2510(12) (1988). *See supra* note 5. Even the business-extension exception to Title III focuses on specified types of equipment. The exception provides an employer a safe harbor only when an employee uses a telephone or telegraph component or facility. *See supra* note 9 and accompanying text.

The proposed Privacy for Consumers and Workers Act also refers to specific types of devices. For example, the Act excludes wiretapping devices as well as the electronic transfer of payroll and other payroll-related information from the definition of "electronic monitoring." H.R. 1218, *supra* note 20, § 2(1)(C); *see also supra* note 93. The proposed Act also excludes electronic data obtained from the use of an electronic card access system and the review of data appearing on multiple television screens from the simultaneous notice requirement.

164. *See* Burnside, *supra* note 31, at 455. Burnside noted that Title III became antiquated within 10 years of its enactment, and asserted that "technological advances occur so rapidly that the laws do not always keep pace to ensure adequate privacy safeguards." *Id.*

illustrate that drafting legislation in terms of specific prohibitions on the employer fails because the legislation interferes with the employer's autonomy.[165] Instead, Congress should draft affirmative legislation which grants employees specific rights.[166] Affirmative legislation will effectively balance the interests of employers and employees.[167]

A. Employees' Affirmative Rights

Fairness of the monitoring process, privacy and autonomy comprise the primary concerns raised by employees with regard to work place monitoring.[168] Congress should draft monitoring legislation that responds to these concerns. First, Congress should retain the provisions of the proposed Act which require an employer to give current and prospective employees actual notice of the specific aspects of the employer's monitoring policy.[169] This provision responds to employees' need for control. If an employee understands the monitoring system, the employee can control her own performance so that it conforms with the employer's requirements.[170]

Second, Congress should require that monitoring employers indicate which devices are monitored by affixing a prominent notice on the actual device.[171] Congress should also mandate that employers provide a sufficient amount of unmonitored telephones or other devices for employees

---

165. *See supra* notes 148-62 and accompanying text.

166. The OTA Report suggested considering "[f]ederal legislation aimed at gaps in current law." The OTA Report described two methods for filling the gaps: (1) general legislation which establishes affirmative rights for employees; and (2) legislation targeted toward specific monitoring practices. *OTA Report*, *supra* note 1, at 22. Congress should enact general legislation granting employees rights within the work place.

167. *See OTA Report*, *supra* note 1, at 22. The OTA Report stated that enacting federal legislation which closes the gaps in current law constitutes one option for legislative reform. The Report provided two possible approaches for structuring the legislation: general legislation which establishes specific rights for employees, or surgical legislation which responds to specific monitoring practices. *Id.* General legislation is the better method because legislation which references specific monitoring practices will inevitably become obsolete. *See supra* notes 164-66 and accompanying text.

168. *See OTA Report*, *supra* note 1, at 1. Generally, most of the employee's concerns relate to the approach employers use to implement monitoring, the use of monitoring to motivate the employees, the manner in which employers use the information and the existence of the monitoring policy. *Id.* at 89.

169. *See* H.R. 1218, *supra* note 20, § 3. *See also supra* note 96 and accompanying text.

170. *OTA Report*, *supra* note 1, at 93.

171. Yet, this provision differs from the simultaneous notice provision of the proposed Act which requires that an employer notify an employee as the monitoring occurs. *See* H.R. 1218, *supra* note 20, § 3(a)(5). *See also supra* note 99. The prominent notice provision advocated by this propo-

to use freely.[172] This provision responds to employees' privacy and control concerns because the employee can decide whether to allow an employer to monitor a personal conversation by choosing the phone on which to place the call.

Finally, the legislation should require employers to prepare and distribute written standards detailing how the employer will use the data obtained by monitoring to evaluate employee performance. These written standards should apply to any supervisor who evaluates other employees on the basis of monitored data.[173] The requirement that employers explain how they will utilize the gathered information addresses concerns of fairness.[174] If an employer is forced to articulate the purposes for using such data, market forces may dissuade an employer from instituting a particularly onerous or abusive monitoring practice.[175] Moreover, objective written standards for evaluation will obviate the problem of supervisors rendering highly subjective evaluations.[176]

B. Defining the Scope of Covered Employers

Congress should avoid defining the scope of protective legislation in terms of specific types of monitoring equipment already in existence.[177]

---

sal merely requires an employer to identify clearly those devices that it monitors. The employer need not indicate when the monitoring actually occurs.

172. *See Hearings on H.R. 1218*, *supra* note 18, at 61 (statement of Richard A. Barton, Senior Vice President, Government Affairs, Direct Marketing Association). Barton argued that in lieu of requiring beep tones, which negatively impact the purposes behind telephone monitoring, Congress should amend H.R. 1218 to require: (1) notification stickers on monitored telephones, and (2) employee access to separate telephones for personal calls.

173. One of the primary allegations of unfair monitoring is "punitive use of monitoring information by supervisors." *OTA Report*, *supra* note 1, at 1.

174. Whether or not monitoring is perceived as reasonable depends on: "(1) the fairness of the standards set, (2) the fairness of the measurement process employed, and (3) the fairness of the way measurements are used in employee evaluation." *OTA Report*, *supra* note 1, at 87.

175. *See id.* at 21. The OTA Report addressed the argument that no congressional action is needed because natural "market forces" limit unfair monitoring. *Id.* If "market forces" will generally dissuade an employer from monitoring unfairly, market forces will likewise dissuade employers from instituting an abusive policy when legislation forces the employer to disclose the unfair or abusive practice.

176. *See supra* notes 173-75.

177. For example, Title III defines "electronic monitoring" in terms of communications transmitted by "wire, radio, electromagnetic, photoelectronic or photo-optical systems." 18 U.S.C. § 2510(12) (1988). Similarly, the proposed Act defines "electronic monitoring" to include the collection of information transmitted by "wire, radio, electromagnetic, photoelectronic or photo-optical system[s]." H.R. 1218, *supra* note 20, § 2(1)(A); *see also supra* note 92. The drafters of the Act did not indicate whether this list is inclusive or merely illustrative.

Such definitions inevitably render any monitoring legislation obsolete because employee monitoring conducted by technologically-advanced devices will eventually fall outside the scope of the legislation.[178] Rather, the legislation should define "monitoring employers" in terms of the act of impersonal observation, rather than by the equipment used to conduct the monitoring.[179] Congress should also specify the standards that an employer must meet when conducting impersonal observation.

C. Provisions of the Proposed Act Which Should be Retained

First, in order to further protect employee privacy, Congress should adopt the provisions of the proposed Act which require an employer to permit employee review of data, which limit disclosure and which prevent monitoring in private places.[180] These provisions provide additional safeguards against abusive monitoring without unduly burdening the employer's ability to manage the work process.[181]

---

178. *See* Burnside, *supra* note 31, at 455 (arguing that technological advances occur so rapidly that the law may not always keep pace).

179. The proposed Act attempts to define "electronic monitoring" in these terms; however, the Act dilutes the scope of coverage by also providing a specific list of the types of transfers which the Act will protect. *See id.* Specifically, the Act states that electronic monitoring covers any "form of visual, auditory, or computer-based technology which is conducted by any method other than direct observation by another person . . ." *Id.*

The broad scope of the protection advocated by this proposal will not unduly restrict an employer, because the affirmative rights granted to the employee do not burden the employer to the extent that the prohibitions of the proposed Act burden the employer. *See supra* notes 153-58 and accompanying text.

180. H.R. 1218, *supra* note 20, §§ 4, 5. *See also supra* note 104.

181. Using the gathered data to discipline an employee illustrates the need for a requirement which will permit an employee to review all the data upon request. When an employer questions the employee regarding an incident which occurred weeks earlier, the employee may be unable to respond adequately to the allegation. *See Hearings on H.R. 1218*, *supra* note 18, at 102 (statement of Tom Higginbotham, General Chairman, International Association of Machinists and Aerospace Workers, AFL-CIO) ("When employees are questioned over conversations that could have taken [place] days, even weeks before, after receiving hundreds of calls in the interim period, it is virtually impossible to respond to false allegations.").

In addition, Congress needs to limit the disclosure of data that the employer gathers by monitoring. In some cases, employers post data for no reason except to humiliate some employees. *See Hearings on H.R. 1218*, *supra* note 18, at 16 (statement of Morton Bahr, President of the Communications Workers of America). Bahr testified that some employers post monitored data conspicuously. Bahr stated: "[S]ome employers post conspicuously the daily time records of employees, showing not only how long it takes for each worker to carry out his or her duties but also the time used for bathroom breaks."

The undue invasion of privacy also concerns employees. *See id.* at 66-67 (statement of Ellen Bravo, Associate Director, 9to5 National Association of Working Women) ("Some common themes emerge, that monitoring too often . . . invades privacy by enabling managers to snoop on personal

Second, to facilitate employers' acceptance of the statute, Congress needs to retain the provision exempting employers from providing specific notice of monitoring where "the employer has a reasonable suspicion that an employee is engaged in conduct which violates criminal or civil law."[182] This provision allows employers to protect against illegal conduct without having to notify suspects that the employer is monitoring their conversation.[183]

D. Enforcement Provisions

Congress should retain all of the enforcement provisions of the proposed Act, including the provisions authorizing civil penalties and private rights of action for employees.[184] However, to enforce the provision requiring employers to establish written standards for evaluation, Congress should create an additional cause of action for an employee who can demonstrate that an employer engaged in a pattern of gross deviation from these standards. This provision will ensure that an employer does not articulate one monitoring policy, and then actually practice a more onerous and abusive policy. Finally, Congress should also adopt the "whistleblower" provision of the proposed Act. The "whistleblower" provision, which prevents an employer from taking any retaliatory action against an employee who brings an action under the legislation,[185] will ensure that employees retain a valid remedy.

CONCLUSION

A basic tension exists between an employer's right to manage the work process and an employee's interest in maintaining autonomy, dignity and privacy in the work place.[186] Neither existing legislation nor the proposed Privacy for Consumers and Workers Act effectively balances these

calls and discussion between co-workers, count time spent in the bathroom and publicly post individual workers' performance.").

182. *See* H.R. 1218, *supra* note 20, § 3(3)(A)(i). *See also supra* note 97 and accompanying text.

183. *See Hearings on H.R. 1218*, *supra* note 18, at 82 (statement of Vincent L. Ruffolo, President of A & R Security). Discussing the simultaneous notice requirement of the proposed Act, Ruffolo acknowledged that the beep requirement puts employers "in the absurd position of having to advise suspected thieves that they are being observed." *Id.* The same logic holds true for requiring employers to give notice of monitoring to employees suspected of illegal activity.

184. H.R. 1218, *supra* note 20, § 7. *See also supra* notes 105-06 and accompanying text. However, the enforcement provisions of the proposed Act are substantially the same as the enforcement provisions contained in Title III. *See* 18 U.S.C. § 2520 (1988).

185. *See* H.R. 1218, *supra* note 20, § 8. *See also supra* note 105 and accompanying text.

186. *OTA Report*, *supra* note 1, at 2.

two interests.[187] Current law fails to delineate any discernable rights between employers and employees.[188] The proposed Act unduly burdens the ability of the employer to manage the work process. Currently, the law contains no requirements that employers conduct "fair" monitoring.[189] Legislation granting affirmative rights to employees mandates fair practices by employers without unduly burdening the management process. Congress should pass legislation granting employees specific rights in the work place.

Susan Ellen Bindler

187. *See supra* note 109 and accompanying text.
188. *See OTA Report, supra* note 1, at 2.
189. *Id.*