Tipping the Balance of Power: Employer Intrusion on Employee Privacy Through Technological Innovation

Patrick Boyd

Follow this and additional works at: https://scholarship.law.stjohns.edu/jcred

Recommended Citation
Available at: https://scholarship.law.stjohns.edu/jcred/vol14/iss2/1

This Note is brought to you for free and open access by the Journals at St. John's Law Scholarship Repository. It has been accepted for inclusion in Journal of Civil Rights and Economic Development by an authorized editor of St. John's Law Scholarship Repository. For more information, please contact lasalar@stjohns.edu.
TIPPING THE BALANCE OF POWER: EMPLOYER INTRUSION ON EMPLOYEE PRIVACY THROUGH TECHNOLOGICAL INNOVATION

Massachusetts senator Edward Kennedy remembers, “I ran for the Senate at a very young age, and one of the issues used by the opponents was that I had never worked a day in my life. One day I was going through one of the factories in my state to meet the workers. And I will never forget the fellow who came up to me, shook my hand, and said, ‘Mr. Kennedy, I understand that you have never worked a day in your life. Let me tell you, you haven’t missed a thing.’”

INTRODUCTION

Though most people need their jobs, it is regrettably rare that they like or love them. Courts and legislatures, with some success, have created statutory and common laws to protect the

---

1 See Bob Dole, Great Political Wit: Laughing Almost All the Way to the White House 25 (Doubleday ed. 1998).
dignity of workers. Technological innovation, however, which permits employers to electronically monitor their workers, now permits employers to compromise their employees by violating their right to privacy in a way not anticipated by earlier laws. Worker integrity and the welfare of the labor force is contingent upon successful management of these new monitoring devices, and the preservation of privacy in the workplace.

Court decisions have provided guidance for recognizing privacy rights in stating that "a guarantee of certain areas or zones of privacy does exist under the Constitution." These rights have origins in the Bill of Rights and the 14th amendment, and have been applied with constitutional justification under the vehicles


4 See Roe v. Wade, 410 U.S. 113, 153 (1973) (arguing that pregnant mother has fundamental right to choose to have abortion); see also Planned Parenthood v. Casey, 505 U.S. 833, 845 (1992) (affirming fundamental right established in Roe with qualified exceptions); Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (establishing right of privacy); Borucki v. Ryan, 827 F. 2d. 826, 838 (1987) (stating that there are zones of privacy under Constitution).

5 See U.S. CONST. amend. 1 (stating that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances"); see also Griswold, 381 U.S. at 486 (establishing Constitutional source of right to privacy); Boyd v. United States, 116 U.S. 616, 621-22 (1886) (invoking 4th and 5th Amendments to prevent government invasion of private residence); Maureen S. Dorney, Privacy and the Internet, 19 HASTINGS COM/ENT L.J. 635, 637 (1997) (stating that privacy rights emanated from Bill of Rights); Mark Silverstein, Privacy Rights in State Constitutions: Model for Illinois?, 1989 ILL. L. REV. 215, 221 (1989) (stating that court in Griswold found support for zone of privacy in Bill of Rights).

of substantive due process\(^7\) and equal protection.\(^8\) The right to privacy, however, can be significantly affected by the context in which it is claimed, and exists only to a limited extent in the workplace.\(^9\) Public sector employees are now granted almost all the rights under the constitution,\(^10\) but unfortunately similar protections have not emerged for private sector workers.\(^11\) This disparity is partially understandable since federal protections do not automatically apply to States or private sector entities.\(^12\) It is


\(^8\) See Loving v. Virginia, 388 U.S. 1, 10 (1967) (holding that statute preventing interracial marriage violated fundamentally private right to choose whom one marries and violated equal protection clause of 14th Amendment); see also Christina Jax, Same Race Marriage - Why Not?, 4 WIDNER J. PUB. L. 461, 485 (1995) (stating that people are afforded same rights under equal protection which includes right to zone of privacy); Michael K. Stinson, Fundamental Rights in the “Gray Area.” The Right to Privacy Under the Minnesota Constitution, 20 WM. MITCHELL L. REV. 383, 411 (1994) (recognizing relationship between equal protection and zone of privacy).

\(^9\) See Hannibal F. Heredin, Is There Privacy in the Workplace?: Guaranteeing Broader Privacy Rights for Workers Under California Law, 22 SW. U.L. REV. 307, 307-08 (1992) (stating that "employees as well as applicants are subjected to a barrage of intrusive tests and monitoring"); Michael F. Rosenblum, The Expanding Scope of Workplace Security and Employee Privacy Issues, 3 DEPAUL BUS. L.J. 77, 78 (stating that "privacy rights of employees must be considered by employers"); see, e.g., McAuliffe v. Mayor & City of New Bedford, 29 N.E. 517, 517 (Mass. 1892) (rejecting claim by stating that "[t]he petitioner may have a constitutional right to talk politics, but he has no constitutional right to be policeman").


\(^11\) See, e.g., Briggs v. American Air Filter Co., 630 F. 2d 414, 420 (5th Cir. 1980) (holding that employer suspecting employee misconduct could listen in on that employees phone calls); Barba, supra note 2, at 902 (discussing limited privacy rights of employees); Heredin, supra note 9, at 78 (stating that employees have limited rights); Mike Tonsing, Privacy in the Workplace, 46 FED. LAW 42, 43 (June 1999) (stating that in most states telephone monitoring is legitimate if done for business purposes). But see Watkins v. L.M. Berry & Co., 704 F. 2d 577, 583 (1983) (holding that simply because employer suspected particular employee was going to quit he could not monitor that employee's calls).

surprising, however, because the earliest form of workplace regulations applied to the private sector.\textsuperscript{13}

The basic purpose of this note is to highlight the lack of privacy protections afforded to private sector employees.\textsuperscript{14} In particular, the Omnibus Crime Control and Safe Streets Act of 1968,\textsuperscript{15} and the Electronic Communications Privacy Act of 1986,\textsuperscript{16} though passed explicitly to protect employee privacy,\textsuperscript{17} allow employers an alarming amount of discretion to intercept the phone conversations and e-mail messages of their employees.\textsuperscript{18} These forms of legislation need further thought and revision to keep pace with technological advances in monitoring equipment and the power these advances give to employers.\textsuperscript{19} Only with appropriate regulation can the integrity of workers and the civility of their relationship with their employers be maintained.

to workers against employment discrimination).

\textsuperscript{13} See, e.g., Wickard v. Filburn, 317 U.S. 111, 119 (1942) (upholding 1938 Agricultural Adjustment Act's quota on farm production even within confines of one farmer's private use of his wheat crop); U.S. v. Darby, 312 U.S. 100, 114 (1941) (upholding Fair Labor Standards Act regulation of private and public sector workers); NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1, 80 (1937) (upholding National Labor Relations Act of 1935 and its challenge to unfair labor practices as within jurisdictional scope of commerce power and thereby subject to monitoring).

\textsuperscript{14} See e.g., Julia Turner Baumhart, The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?, 8 LAB. LAW. 923, 923 (1992) (stating that reading electronic messages may violate employee privacy rights); Gantt \textsuperscript{ supra} note 3, at 345 (observing that because of sophisticated nature of contemporary workplace monitoring “modern offices are becoming electronic sweatshops”).


\textsuperscript{17} See U.S. v. Giordano, 416 U.S. 505, 514 (1974) (stating Act's goal was to be to prohibit “all interceptions of oral and wire communications except those specifically provided for in the act”); U.S. v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974) (holding that protection of employee privacy is basic purpose of “Act”); see also Carol M. Bast, What's Bugging You? Inconsistencies and Irrationalities of the law of Eavesdropping, 47 DEPAUL L. REV. 837, 842 (1998) (stating that legislation was passed “to prevent the interception of oral and wire communications without the consent of at least on party”).


\textsuperscript{19} See Giordano, 416 U.S. at 515 (stating that technological require caution in permitting wiretapping); see also Richard D. Mark, High Technology Legislation as an Eighteenth Century Process, 6 STAN. L. POLY REV. 17, 18 (1994) (stating that “scientific innovation does not slow to allow judges and legislators to keep pace”). But see Patricia M. Worth, The Impact of New and Emerging Telecommunication Technologies: A Call to the Rescue of the Attorney Client Privilege, 39 HOWARD L.J. 437, 454 (1996) (stating that Congress' “effort to keep pace with technological advancements evinces a steadfast commitment to technology”).
Part I of this note provides a description of the advantages that employers have over employees in establishing employment contracts. These advantages suggest that employees are ill-equipped to defend their privacy interest for fear of losing their jobs and highlight the need for statutory protection. Part II discusses the Omnibus Crime Control and Safe Streets Act of 1968 and Part III discusses the Electronic Communications Privacy Act of 1986. These statutes were designed in part to protect the privacy of workers and their relative success will be considered in some detail.

I. THE WORKPLACE BALANCE OF POWER

To understand the danger of unregulated employee monitoring more concretely, the different goals of employers and employees in the employment relationship must be considered. Employers seek maximum efficiency and earnings, and view the monitoring of phone and e-mail use by employees as a way to "maintain production standards, spot bottlenecks, and plan personnel and equipment needs."20 One court, in recognizing this need, elaborated on its importance by remarking "[i]nterception of calls reasonably suspected to involve non-business matters might be justifiable by an employer who has had difficulty controlling personal use of business equipment through warnings."21 Employees, on the other hand, seek higher wages, benefits, and dignity. They find monitoring of their phone and computer communications intrusive and unnecessary.22

Satisfying the competing needs of employers and employees is difficult because employees are almost always at a disadvantage and therefore unable to protect their privacy interests.23 It is true

21 See Briggs v. American Filter, Co., 630 F.2d 414, 420 n.8 (5th Cir. 1980). The court in this case was also concerned with the need of employers to maintain confidentiality with respect to certain trade secrets. Id. at 420.
22 See OFFICE OF TECHNOLOGY ASSESSMENT, supra note 20, at 8 (stating that "[t]wo major objections to electronic monitoring of individual performance are allegations that it contributes to employee stress and stress related illness and that it contributes to an atmosphere of distrust is the workplace"); see also Heredin, supra note 9, at 307-08 (explaining how employees can be exposed to distressful and intrusive tests).
23 Though this inequity is widely recognized. It should be noted that government intervention is more frequent when the work relationship affects commerce. To quote from the landmark case, NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1, 80 (1937),
that no law requires employers to hire any particular worker or any workers at all, nor are employees required to work, but employers are more likely to have additional job applicants than prospective employees are to have additional jobs opportunities. Often, then, an employment contract is presented and accepted on terms that are not of the employee's choosing.24

Once an employment contract is created the problem is compounded because it is less likely that employees will bring suits to protect their privacy interests. First, the labor market is flooded with workers and employees may be willing to sacrifice their rights for a much needed job. Also, litigation costs are more difficult for an employee (as opposed to an employer) to absorb, which serves as a disincentive to bringing privacy suits.25 Additionally, the situation is difficult because employees willing to challenge monitoring may not be aware that their privacy is being violated, as technology conceals the monitoring from their observation.26

As Americans spend a disproportionate amount of their lives working, it is essential that their workplace rights are protected.27 Without suitable laws to ensure such protection permitting government intervention: "[I]t is idle to say that the effect of labor strife on commerce would be indirect or remote. It is obvious that it would be immediate and catastrophic. We are asked to shut our eyes to the plainest fact of our national life and to deal with questions of direct and indirect effects in an intellectual vacuum. [Industrial strife] is a matter of the most urgent national concern." \(\text{Id.}\) See also Mark A. Rothstein, Wrongful Refusal to Hire: Attaching the Other Half of the Employment-at-Will Rule, 24 CONN. L. REV. 97, 117 (1991). The author suggests exceptions to the employment-at-will approach because of the inequality in bargaining power of the parties. \(\text{Id.}\)

24 See e.g. Steven L. Wilborn et al., Employment Law Cases and Materials (Lexis Law Publishing 2d ed. 1993) (demonstrating bargaining disadvantages of employees).

25 See Stefan Rutzell, Snitching for the Common Good: In Search of a Response to the Legal Problems Posed by Environmental Whistleblowing, 14 TEMP. ENVTL. L. & TECH. J. 1, 50 (1995) (stating that [t]he high costs associated with litigation may deter an employee from going to court).\(\text{Id.}\)

26 See Gantt, supra note 3, at 346-47 (stating that employers can invade employees privacy with little or no detection).

27 See Cynthia Estlund, Freedom of Expression in the Workplace and the Problem of Discriminatory Harassment, 75 Tex. L. Rev. 687, 734 (1997) (stating that workplace should be recognized as important forum for discussion); see also Mark Barenberg, Democracy in the law of the Workplace Cooperation: From Bureaucratic to Flexible Production, 94 Colum. L. Rev. 758, 761 (1994) (proposing empowerment of employees through various programs including in-house participatory and representative schemes); Terry S. Boone, Selected Topics on Employment & Labor Law: Violence in the Workplace and the New Right to Carry Gun Law - What Employers Need to Know, 37 Tex. L. Rev. 873, 874 (1996) (stating that employer has obligation to protect employee); David Weil, Are Mandated Health and Safety Committees Substituted For or Supplements to Labor Unions?, 52 IND. & LAB. REL. REV. 339, 340 (1999) (stating work councils, labor
them, they are bound to be exploited by their employers. They need their jobs and will not risk them to solve inequities, but new technological developments have outpaced the existing sources of privacy protection and have grossly shifted the balance of power between employers and employees. One professor explained how the employment contract in such a context is becoming more akin to a contractual relationship of adhesion:

These new monitoring technologies have intensified employee privacy concerns because the instruments abolish the desirable balance of power between employers and employees. The instruments allow employers to invade the personal lives of employees with little or no chance of detection. Furthermore, electronic monitoring allows employers to manipulate, access, and collect information about employees in greater amounts than reasonably possible.

Two acts were designed to prevent this type of exploitation. Each will be considered in some detail below.

management committees and other forms of worker participation can improve employee involvement in workplace).

This was not the early conception of employment contracts. For example, in Adair v. United States, 208 U.S. 161, 174-75 (1908) the Court advocated a mutuality of obligation between the employer and employee whereby the employer could fire the employee for any time at any reason and the employee could quit at any time for any reason. After the Lochner Era, however, the courts began to acknowledge the inherent weakness of employee bargaining power. See, e.g., Chiodo v. General Waterworks Corp., 413 P. 2d. 891, 894 (1966) where the court held that equitable principles demanded good faith from the employer. See generally Sarah G. Burns, Evidence of a Sexually Hostile Workplace: What is it and how Should it be Assessed After Harris v. Forklift System, Inc., 21 NYU Rev. L. & Soc. Change 357, 415 (1994). The author notes that the Supreme Court has stated that it restricted employer activities which exploited the employee power deficiency. Id.

See Gantt, supra note 3, at 345 (summarizing concerns about technological advances in employer monitoring capabilities); see also Rod Dixon, Windows Nine-to-Five: Smyth v. Pillsbury and the Scope of an Employee’s Rights of Privacy in Employer Communications, 2 VA. J.L. & Tech. 4, 4 (1997) (discussing impact of computer communication technology in workplace); Peter Schnaitman, Building a Community Through Workplace E-mail: The New Privacy Frontier, 5 Mich. Telecom. Tech. L. Rev., 177, 177 (1999) (suggesting that technology of e-mail presents new issue of workplace privacy); Scott A. Sundstrom, You’ ve Got Mail (And the Government Knows it): Applying the Fourth Amendment to Workplace E-Mail Monitoring, 73 N.Y.U. L. Rev. 2064, 2064 (1998) (stating that workplace e-mail monitoring is increasing because it is simple for employers to use on large scale).
II. THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968

The Omnibus Crime Control & Safe Streets Act of 196830 (hereinafter "the Act") is a federal act that was constructed, in part, to protect the integrity and privacy of employees in the workplace.31 Title III of the Act has significant penalty provisions,32 and regulates wiretapping and eavesdropping by private individuals and governmental entities.33 In United States v. Giordano et al.,34 the Supreme Court provided a useful definition of the Act’s purpose stating: “The purpose of the legislation, which was passed in 1968, was effectively to prohibit,

31 See Janet Booth Jones, Annotation: Application to Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 Pertaining to Interception of Wire Communications, 58 A.L.R. FED 594, 598 (1998) (discussing application of Act in a workplace context); Todd R. Smyth, Eavesdropping on Extension Telephone As Invasion of Privacy, 49 A.L.R. 4TH 430, 451 (1999) (discussing the Act and employees' right to privacy); see also Carol M. Bast, supra, note 18, at 842 (1998) (stating that the Act was designed to prevent interception of wired conversations without the consent of at least one party).
In general ... 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.
Relief - In an action under this section, appropriate relief includes—such preliminary and other equitable or declaratory relief as may be appropriate; damages under subsection (c) and punitive damages in appropriate cases; and a reasonable attorney's fee and other litigation costs reasonably incurred.
See also Janet Booth Jones, supra note 31, at 825 (noting that Act has provisions for criminal and civil penalties);
33 See 18 U.S.C. §2511(1)(a) (1994). §2511(1)(a) generally prohibits the use of wiretapping and eavesdropping. §2511(1)(a) states that:
(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, any wire, oral or electronic communication; ... shall be punished as provided in subsection (4) or shall be subject to a suit as provided in subsection (5).
on the pain of criminal and civil penalties, all interceptions of oral and wire communications, except those specifically provided for in the Act.”

Although on its face the language of the Act appears broad enough to curtail employer exploitation of employee privacy, it fails in several respects. Most importantly, the Act has exceptions to its general prohibition on wiretapping, which undermine the privacy expectations of employees. These

35 Id. at 514; see also Jones, supra note 31, at 598 (stating purpose of statute is to prohibit the secret monitoring or wire communications).

36 See Smythe, supra note 31, at 436 (stating that Act now provides remedy for privacy invasion); Paul F. Gerhart, Employee Privacy Rights in the United States, 17 COMP. LAB. L. 175, 176 (1995) (noting that Title III “particularly shield[s] private sector employees from employer invasion of privacy”); see also Gantt, supra note 3, at 347 (stating that statute has language that seems sufficient to protect privacy interests).

37 See S. Rep. No. 541, 99th Cong., 2d Sess.; see also Julia Turner Baumhart, The Employer’s Right to Read the Employee E-Mail: Protecting Property or Personal Prying?, 8 LAB. LAW. 923, 924 (1992) (stating that Title III was amended by ECPA to “atone for what Congress saw as deficiencies in individual privacy protections”); Jose L. Nunez, Regulating the Airwaves: The Governmental Alternative to Avoid the Cellular Uncertainty on Privacy and the Attorney Client Privilege, 6 ST. THOMAS L. REV. 479, 485 (1994) (stating that purpose of ECPA was acknowledgement by Congress of need “to update and clarify the Federal privacy protections and standards in light of the dramatic changes in new computer and telecommunications technologies”).


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 tortuous act in violation of the constitution of laws of the United States or of any state.

Id.

§2510(5)(a) is a business telephone exception providing that:

Electronic, mechanical, or other device does not include: 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 or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business.

See also Jones, supra note 31, at 600. There, the author notes that in United States v. Sturdivant, 9 M.J. 923 (1980), the court held that the first sergeant’s use of extension phone to intercept phone call between members of his battery was in ordinary course of business and came within statute’s exception in section 2510(4).

Id. David Neil King, Privacy Issues in the Private Sector Workplace: Protection From Electronic Surveillance And the Emerging Privacy Gap, 67 CAL. L. REV. 441, 451 (1994). The author notes that under the Act, in a prima facie case, the defense may rebut the plaintiff’s evidence or raise defenses or exceptions. Id.

39 See Gantt, supra note 3, at 345 (summarizing concerns about technological encroachments on employee privacy); Jones, supra note 31 at 598 (discussing interception of conversation between members of police and narcotics bureaus). Cf. Omnibus Crime Control and Safe Street Act of 1968, S. Rep. No. 1097, 9th Cong., 2d Sess. 68, reprinted in 1968 U.S. CODE CONG. AND AD. NEWS 2153, (noting that Title III was enacted to enhance the privacy of wire and oral communications).
exceptions are known as the consent exception and the business extension telephone exception, and will be considered in some detail below.

A. The Consent Exception to the Omnibus Crime Control and Safe Streets Act of 1968

The consent exception to the Omnibus Crime Control and Safe Streets Act of 1968 permits employers to intercept employee phone calls "where such person is a party to the communication or where one of the parties to the communication has given prior consent." The courts have thus far held that the consent for these interceptions may be actual or implied, and can be "inferred from surrounding circumstances." Court decisions have further indicated that the consent requirement is to be construed broadly, not casually, and that liability will not attach to employers because of inadvertent interceptions.

The consent exception was interpreted by the First Circuit to serve as a safe harbor for those who intercept phone calls without

---

42 See 18 U.S.C. §2511(2)(d) (1994); see also U.S. v. Shields, 675 F.2d 1152, 1156 (11th Cir. 1982) (discussing application of consent exception); U.S. v. Mendoza, 574 F.2d 1373, 1377 (5th Cir. 1978) (referring to consent exception); U.S. v. Ransom, 515 F.2d 885, 889 (5th Cir. 1975) (explaining consent exception).
43 See United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996) (stating that "[c]onsent may be either express or implied"); United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987) (noting that consent may either be expressed or implied under Title III).
44 See, e.g., Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993) (stating "implied consent is 'consent in fact' which is inferred 'from surrounding circumstances indicating that the party knowingly agreed to the surveillance" (quoting Amen, 831 F.2d at 378)); U.S. v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1995) (stating consent may be express or may be implied in fact from "surrounding circumstances indicating that the [defendant] knowingly agreed to the surveillance).
45 See, e.g., Gilday v. Dubois, 124 F.3d 277, 296 (1st Cir. 1997) (noting that "'consent' exception under Title III is 'construed broadly' as encompassing implied consent" (citations omitted)); Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (agreeing with Second Circuit that "Congress intended the consent requirement to be construed broadly" (quoting Amen, 831 F.2d at 378)); United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996) (stating "[t]he legislative history [of Title III] shows that Congress intended the consent requirement to be construed broadly" (quoting Amen 831 F.2d at 378)).
46 See, e.g., United States v. Townsend, 987 F. 2d 927, 930 (2d Cir. 1993) (holding that in Title III claims defendants act must have been product of defendant's conscious objective rather than product of mistake or accident); Forsyth v. Barr, 19 F.3d 1527, 1534 (5th Cir. 1994) (noting that "the wording of the statute [Title III], while broad, requires that interceptions be intentional before liability attaches, thereby excluding inadvertent interceptions"(quoting Thomas v. Dulaney, 907 F.2d 744, 748 (10th Cir. 1992)); see also Watkins v. L.M. Berry & Co., 704 F.2d 577, 581-85 (11th Cir. 1983) (discussing notion of inadvertent interception in the workplace).
explicit consent. In *Griggs-Ryan v. Smith*,47 for example, the plaintiff was a tenant at a campground which the defendant, Smith, operated.48 Lodgers at the grounds were permitted to use Smith's telephone and were informed that their conversations were being taped by Smith, who was attempting to record obscene calls she had been receiving.49 On the day in question, Smith answered the phone and gave it to plaintiff (as the call was for him).50 Smith was about to hang up the phone when she heard what she suspected to be information about a drug conversation.51 She opted to tape the conversation and the plaintiff was arrested following a search of his house.52

The court found that Smith's behavior was protected under the consent exception to Title III and that her taping was permissible.53 The court explained that the plaintiff was acting at his own risk since Smith never informed him that she would stop monitoring calls once she determined they were not harassing.54 In *United States v. Amen*,55 the Second Circuit reached a similar conclusion when the court held that the consent exception permitted evidentiary use of phone tapes made in a prison because the prisoners had received jail house handbooks alerting them to the prison's recording procedures.56

In the context of workplace privacy, the consent exception retains the same legal character. In *Deal v. Spears*,57 a United States District Court considered whether employer taping of

47 904 F.2d 112 (1st Cir. 1990).
48 See Griggs at 114.
49 See id.
50 See id.
51 See id.
52 See id.
53 See id. at 119.
54 See id. at 117 (noting that plaintiff offered no evidence suggesting that he had not given consent to taping of call).
55 831 F.2d 373 (2d Cir. 1987).
56 See id. at 379-80 (holding that reading of handbooks constituted consent); see also U.S. v. Workman, 80 F.3d 688, 693 (2d Cir. 1996)(explaining *Amen* decision); People v. Goldfeld, 400 N.Y.S. 2d 229, 234 (N.Y. App. Div. 1977) (stating where one party had consented to taped telephone conversation tape recording was not considered "intercepted communication" within Act); Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private Sector Employers to Read Their Employees' E-Mail?*, 20 HAWAII L. REV. 165, 205-06 (1998) (applying consent exception to email). *But see* Crooker v. U.S. Dept. of Justice, 497 F. Supp. 500, 503 (D. Conn. 1980) (holding that prisoners' knowledge of call monitoring did not constitute consent).
employee calls would be exempt from violating the Act, when the employer had threatened that he “might” put in a pay phone or “monitor” employee calls.\(^{58}\) The court, applying a standard reminiscent of those in Griggs and Amen, held that an employer’s threats to use a phone tap were not sufficient to imply consent of the employee.\(^{59}\) In Ali v. Douglas Cable Communications,\(^{60}\) a District Court considered a case in which an employer monitored employee phone calls, and “did not distinguish between business or personal calls.”\(^{61}\) Though the employer had posted and distributed office notices about phone monitoring,\(^{62}\) the court held that consent had not been established sufficiently for a motion for summary judgement to be granted for the defendant,\(^{63}\) suggesting that consent was not clearly established because the employer did not have a formal monitoring procedure which the plaintiffs knew about.\(^{64}\)

Though the disposition of these cases is consistent and fair, two key points should be kept in mind. First, after establishing consent or notifying an employee, an employer is free to monitor

\(^{58}\) See id. 622.

\(^{59}\) See id.; see also David Neil King, Privacy issues in the Private Sector Workplace: Protection from Electronic Surveillance and the Emerging Privacy Gap, 67 S.CAL. L.REV. 441, 454 (1994) (stating that Deal was one of first cases to apply Griggs doctrine in employment law context). See generally Kevin P. Kopp, Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy, 8 SETON HALL CONST. L.J. 861, 882-83 (1998) (stating that consent exception was considered in Deal).


\(^{61}\) See id. at 1373. These calls were monitored because the defendant company engaged in telephone customer service. Id. The calls were intended to be monitored for training purposes. Id.

\(^{62}\) Id. at 1373 (noting that “[s]ome of the [employees] knew of the telephone monitoring because the supervisors had used it during their training, and other [employees], like the plaintiffs were not aware of it”).

\(^{63}\) Id. at 1378 (holding that “a telephone extension used without authorization or consent to record a private conversation” is not exempt from Act).

an employee's phone calls. While this employer prerogative alone is disturbing, consider scenarios in which the only phone available to the employee is in the place of business. Should an employee be required to accept that all his or her calls from work are being monitored by their employer? Second, there is a distinct probability that many employers are monitoring their employees without their knowledge or consent.

Though the act does grant employees statutory damages when their privacy rights have been compromised, it is unlikely that these penalties serve as a deterrent for an employer who runs the risk of being caught.

B. The Title III Exemption for Business Extension Telephones

The second exception to the Omnibus Crime Control and Safe Streets Act is provided in §2510(5)(a). This section excludes equipment "furnished to the subscriber... by a provider in the ordinary course of its business and being used by the subscriber in the ordinary course of its business." This exemption is commonly referred to as the "extension telephone exemption."
The hallmark case in defining the limits of this exception is *Watkins v. L.M. Berry.* In *Watkins,* the defendant, Berry Company, had a policy of monitoring the solicitation of its employees as part of its training program. The monitoring was done with an extension telephone, which employees were told that they could use to make unmonitored personal calls. Watkins used the phone to discuss an upcoming employment interview with a friend and the call was monitored despite the company's policy. When Watkins' supervisor discovered her intentions to seek new employment through the phone extension he confronted her and she was fired. The court held that a personal call cannot be intercepted in the ordinary course of business except for the employer to determine whether or not it is personal. It reversed the lower court grant of summary judgement to the employer, remanding the case to determine whether Watkins had given her consent to the call monitoring.

The *Watkins* court expressed concern at how the course of the business exception had been used in certain cases. It cited and critiqued a decision in the Tenth Circuit which held that a three-to-five minute call interception which resulted because the conversation "sounded interesting" was not in violation of the Act because it was not "willful" within the meaning of the statute. In *Epps v. St. Mary's Hospital of Athens, Inc.,* the conversation called "extension telephone exception").

---

73 704 F.2d 577 (11th Cir. 1983).
74 See id. at 579.
75 See id.
76 See id.
77 See id.
78 See id. The plaintiff later complained to her supervisor and was reinstated with apologies. A week later she began work at her new job. *Id.*
79 See id. at 583 (stating that reasonable allowance of time is to be given to employers to establish nature of call); see also United States v. Savage, 564 F.2d 728, 732 (5th Cir. 1977) (holding listening to call for 10-15 seconds was permissible because operator was elderly). But see United States v. Axelle, 604 F.2d 1330, 1335 (10th Cir. 1979) (holding that 3-5 minute interception was excusable).
81 See *Watkins,* 704 F.2d at 584-85.
82 See U.S. v. Axelle, 604 F.2d 1330, 1335 (10th Cir. 1979) (describing its reaction to decision as "less enthusiastic" because "[i]t absolutely contradicts the meaning of the operative language (in the statute)"); C.f., U.S. v. Paul, 614 F.2d 115, 117 (6th Cir. 1980) (allowing routine monitoring for security reasons); U.S. v. Savage, 564 F.2d 728, 732 (5th Cir. 1977) (permitting overhearing due to operator's age).
83 802 F.2d 412 (11th Cir. 1986).
EMPLOYER INTRUSION ON EMPLOYEE PRIVACY

of an employee in a hospital emergency room was recorded which contained disparaging comments about a hospital supervisor.\textsuperscript{84} Consistent with the Tenth Circuit's decision, this court held that such gossip constituted business interests of the employer.\textsuperscript{85}

Unfortunately, the court's holdings with regard to this exception are rather unclear. How can the interception of calls about career moves be considered "personal" and violative of the statute, while employee gossip about a boss is determined "business related" and interceptable?\textsuperscript{86} This flaw subjects employee privacy rights to an unjust relativity.\textsuperscript{87} Employees willing to attempt suits with such precarious precedents usually need proof that the employer recorded personal employee phone calls.\textsuperscript{88} As the business extension telephone exemption does not require employee consent when taping occurs one can not help but wonder how any employee can protect himself from abuse. How might an employee check the discretion of employer tapping if it does not recognize its existence?

III. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

In 1986, Congress Amended the Omnibus Crime Control and Safe Street Act of 1968\textsuperscript{89} to compensate for deficiencies in the privacy protections of this act in lieu of new technology.\textsuperscript{90} The amendment was intended, in part, to bring E-Mail and voicemail

\textsuperscript{84} See id. at 413 -14.

\textsuperscript{85} See id. at 417.

\textsuperscript{86} See Frank C. Morris, Jr., Privacy and Defamation in Employment, SB 42 ALI-ABA 201, 219-20 (1997) (discussing inconsistency in court definitions of the employers "ordinary course of business").

\textsuperscript{87} See, e.g., Frank T. Cavico, Invasion of Privacy in the Private Employment Sector: Tortuous and Ethical Respects, 30 HOUS. L. REV. 1263, 1345 (1993) (suggesting that employee rights to privacy should be balanced by courts against the employer's right to run business effectively); Pauline T. Kim, Privacy Rights, Public Policy and the Employment Relationship, 57 OHIO ST. L. J. 671, 706, 729 (1996) (discussing risks employees take in resisting monitoring practices because of the complex standard).

\textsuperscript{88} See, e.g., Ali v. Douglas Cable Communications, 929 F. Supp. 1362, 1380 (D. Kan. 1996) (dismissing complaint because plaintiff could not produce material indicating that personal information was taped).


\textsuperscript{90} See e.g., Baumhart, supra note 14, at 924 (stating that impetus for "Act" was increased threat to civil liberties by unregulated electronic privacy intrusions). See generally Richard M. Schall, Employee Privacy Rights, 581 PLI/LIT 865, 871 (1998) (noting that special needs of employers [to monitor employees] have been satisfied by new technologies).
within the Act's purview. The Amendment, entitled the Electronic Communications Privacy Act (hereinafter "the EPCA"), added to Title III's prohibitions the unauthorized interceptions of electronic communications with the acknowledgement that an individual's interests in his private communication does not change based on the medium used. For purposes of clarification communications protected in the act are defined as "[A]ny transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate commerce."

Facts indicate that the EPCA was a long time in the coming as recent estimates speculate that more than 20 million Americans regularly use E-Mail at work, and that 66 percent of all workers are subject to electronic monitoring by their employers. In one scholar's mind the adoption of this statute might be too late because the monitoring of E-mail is already established:

As technology develops in sophistication, however, commentators debate whether modern technology has given the employer so much control over the workplace that the balance of power between employees and employers must be readjusted by law to ensure adequate employee privacy. The new technologies have thus generated a fundamental uncertainty concerning the privacy rights of employees, as the freedom from monitoring by one's employer is increasingly perceived as being outside the scope of

91 See Baumhart, supra note 14, at 924 (stating that statute "needed broadening" to bring e-mail into its purview); see also Robert B. Fitzpatrick, Technology Advances in the Information Age: Effects on Workplace Privacy Issues, SC 08 ALI - ABA 599, 603 (1997) (concluding that employers are [now] required to obtain employee consent before monitoring e-mail).
93 See Baumhart, supra note 14, at 925 (explaining that EPCA focuses on e-mail communications).
95 See Steven B. Winters, Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail, 1 S. CAL. INTERDISCIPLINARY L.J. 85, 87 (1992) (citing various modern workplace statistics); see also Paul F. Gerhart, Employee Privacy Rights in the United States, 17 COMP. LAB. L.J. 175, 175 (1995) (citing survey indicating that 22% of 301 American Companies reported searching employee communication filed and estimating that 20 Million workers are subject to monitoring); Thomas R. Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 AM. U. L. REV. 219, 222 n. 9 (1999) (noting that 66.2% of employers responding to survey who monitor employees do not notify them of this practice).
96 See Gantt, supra note 3, at 346.
reasonable privacy expectations. [citations omitted]\(^97\)

Because the EPCA is simply an amendment to the Omnibus Crime Control and Safe Streets Act,\(^98\) it is subject to the same exceptions discussed above, and runs similar risks of permitting invasions of employee privacy. At this time, however, few federal cases have explicitly applied the EPCA to an e-mail issue.\(^99\) In *Steve Jackson Games v. United States Secret Service*,\(^100\) the plaintiff operated a computer bulletin board for testing games.\(^101\) One of the plaintiff’s employees was allegedly accessing software illegally, and the Secret Service seized all related computers.\(^102\) The court awarded damages to the plaintiffs, wading through the complexities that new technologies present to older statutes before reaching its conclusion.\(^103\)

One can only speculate what future changes might evolve in the new world of internet technology. The hardware of computers is even more complex than that of phones, so employees are even less likely to detect employer intrusions into this form of communication.\(^104\) This increases the opportunity for employer exploitation, and demands a closer look at the EPCA. It is clear, however, that E-mail will be a new battleground for employee privacy rights.

IV. CONCLUSION

The traditional employment relationship favors the employer and Congress attempted to create a number of federal statutes to protect the interests of workers. The new wave of technology has

---

97 See Gantt, *supra* note 3, at 346.
99 See Davis v. Gregory, 111 F.3d 1472, 1475-76 (10th Cir. 1997) (discussing suit brought by defendant against officers who searched his computer); *Steve Jackson Games v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994) (discussing case where Secret Service seized plaintiff’s computers); see also Bast, *supra* note 17, at 850-51 (describing Steve Jackson Games as only e-mail interception court case).
100 36 F.3d 457 (5th Cir. 1994).
101 See id. at 458.
102 See id. at 459.
103 See id. at 464 (holding that seizure did not violate Federal Wiretap Act).
104 See Sarah E. Burns, *Evidence of a Sexually Hostile Workplace: What is it and How Should it be Assessed After Harris v. Forklift Systems, Inc.*, 21 NYU REV. L. & SOC. CHANGE 357, 415 (1994) (noting Supreme Court case restricting employer activities exploiting employer - employee power deficiency); Gantt, *supra* note 3, at 349 (observing technological complexities of E-Mail and unliklihood that employees will know that theirs is monitored)
brought the workplace to yet another ground of tension between worker and employee interests. At present, the privacy provisions of the Omnibus Crime Control and Safe Streets Act and its amendment are insufficient to face this challenge. Either a new form of privacy protection must evolve or an unfortunate new world order of monitoring and privacy will be instituted. . . and people will hate their jobs more than ever.

Patrick Boyd