NOTE

E-MAIL DISCLOSURE TO THIRD PARTIES IN THE PRIVATE SECTOR WORKPLACE

Jeremy U. Blackowicz [*]

I. INTRODUCTION
II. BACKGROUND
III. E-MAIL PRIVACY PROTECTIONS UNDER THE ECPA
  A. *E-mail Protection Under Title I and Title II of the ECPA*
  B. *Statutory Exceptions to Title I and Title II of the ECPA*
    1. Provider Exception
    2. Ordinary Course of Business Exception
      a. *Context Approach*
      b. *Content Approach*
    3. Prior Consent
    4. Interstate Commerce Requirement
IV. THE PROBLEM OF DISCLOSURE TO THIRD PARTIES
  A. *Disclosure Under Title I*
  B. *Disclosure Under Title II*
V. PROPOSALS TO PROTECT EMPLOYEE PRIVACY
  A. *Employer Monitoring Policies*
  B. *Judicial Interpretation of Current Law*
  C. *Statutory Reform*
VI. CONCLUSIONS

I. INTRODUCTION

Electronic mail[1] ("e-mail") has become an indispensable tool of modern business.[2] It allows rapid exchange of information and surmounts traditional

[*] B.A., *summa cum laude*, 1998, University of Minnesota; J.D. (anticipated), 2001, Boston University School of Law.

[1] E-mail is the electronic equivalent of a paper letter or telephone call, transmitted instantaneously from one computer to another. *See* Reno v. ACLU, 521 U.S. 844, 851 (1997); JOHN R. LEVINE & CAROL BAROUDI, INTERNET FOR DUMMIES 11 (1st ed. 1993). E-mail has become one of the most widely used communications services in the world. *See id.*

[2] *See* Louise Ann Fernandez, *Workplace Claims: Guiding Employers and Employees Safely Through the Revolving Door*, *in* 26TH ANNUAL INSTITUTE ON EMPLOYMENT LAW, at 775, 790, 833 (PLI Litig. & Admin. Practice Course Handbook Series No. H4-5272, 1997)

boundaries to communication. However, the e-mail revolution has its dark side. Employers are better able to monitor their employees surreptitiously. Employers are reading e-mail messages and disclosing them to others without their employee's knowledge or consent. E-mails containing an employee's personal information are being disclosed to others both within and outside the company. Moreover, current law offers inadequate protection from this violation of privacy.[3]

This note examines the current federal privacy protections offered to private sector employees against disclosure of e-mail messages. Part II provides a background analysis of current e-mail use, dangers and protections. Part III examines the history, application, and protection offered by the Electronic Communications Privacy Act of 1986 ("ECPA") to private sector employees against monitoring of their e-mail. Part IV analyzes the problem of e-mail disclosure to third parties and the applicability of the ECPA to this issue. Part V suggests several proposals designed to further the goal of employee privacy by restricting or prohibiting employer disclosure of employee e-mail to third parties. These proposals include strict employer e-mail policies, novel judicial interpretation of the ECPA to address disclosure of employee e-mails, and legislation.

II. BACKGROUND

E-mail has become a prominent and useful form of communication for employees in the private sector workplace.[4] E-mail facilitates and improves communications between co-workers and clients due to its almost instantaneous transmission and ability to transcend geographical areas.[5]

(noting the importance of the Internet to the modern workplace).

[3] *See infra* Section IV (discussing the application of current law to disclosure of e-mail contents).

[4] *See* Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L. REV 139, 139 (1994) (noting that e-mail is the "fastest growing form of electronic communication in the workplace"); Steven B. Winters, Note, *Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail*, 1 S. CAL. INTERDISC. L.J. 85, 87 (1992); *see also Most Workers Optimistic About Technology*, NUA INTERNET SURVEYS, Feb. 22, 2000, *available at* <http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905355610&rel=true> (finding that 80 percent of workers surveyed use e-mail at work); *Net Used Twice as Much in Work as at Home*, NUA INTERNET SURVEYS, Feb. 21, 2000, *available at* < http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905355606&rel=true> (explaining that the 32.7 million workers who have Internet access at work spend twice as much time on the Internet at work compared to home usage, averaging 21 hours a month); *U.S. Internet Users Surpass 100 Million Mark*, N.Y. TIMES, Nov. 10, 1999, *available at* <http://www.channel.nytimes.com/1999/11/10/technology/10net.html> (finding that 69 percent of employees send more than six e-mails each day).

[5] *See* Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 951 (C.D.

Additionally, "e-commerce" businesses are almost exclusively using e-mail for communication with clients.[6] Furthermore, "telecommuting" has become more popular; employees are working from home or mobile locations and sending completed work and messages back to the company through e-mail.[7]

With the number of employees using e-mail on the rise, companies are increasingly interested in controlling the use and content of e-mail messages. To achieve these ends, employers often monitor the messages sent to and from employees.[8] Employers may have a legitimate fear of losing company secrets, a desire to gain insight into employee morale, or a need to apprehend employees who are conducting illegal activities through e-mail.[9] Employers may also justify monitoring on the ground that they have an interest in the job performance and tasks completed by employees who are using company equipment and time.[10] However, there are concerns that employers may monitor e-mail for reasons unrelated to business, thereby violating employee privacy without justification.[11]

Ca. 1997) (noting the Internet's effect of increasing the ability to communicate and share information); Lee, *supra* note 4, at 140; Note, *Addressing the Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1909 (1991).

[6] "E-commerce" is the buying and selling of goods and services solely through the Internet, with all communications occurring by e-mail, fax, and occasionally telephone. *See E-commerce*, WHATIS, Oct. 25, 2000, *available at* <http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,242029,00.html>.

[7] *See Telecommuting/Telework*, WHATIS, Nov. 16, 2000, *available at* <http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,213115,00.html>.

[8] *See* Lee, *supra* note 4, at 141; S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 825-26 (1998); Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1260-62 (1994) (noting that current technology allows secret and continuous monitoring of employees by employers); Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 221 (1994) (noting that new communications technologies have expanded the ways in which an employer may monitor employees without their knowledge).

[9] *See* Flanagan, *supra* note 8, at 1260-62 (discussing the benefits to employers that electronic monitoring may provide); Lee, *supra* note 4 at 144-45; Anne L. Lehman, Comment, *E-mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMMLAW CONSPECTUS 99, 109-10 (1997) (discussing various ways in which an employer may be liable for criminal acts conducted by employees through e-mail); Jarrod J. White, Comment, *E-Mail@Work.Com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1079-80 (1997) (warning that employee misuse of e-mail may lead to employer liability for criminal actions by the employee).

[10] *See* Lee, *supra* note 4, at 145; Winters, *supra* note 4, at 95-96; Lehman, *supra* note 9, at 99.

[11] *See* Larry O. Natt Gantt II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 346 (1995) (noting that employers are able to invade employee privacy with little chance of detection and access or

Employees are often unaware of the employer's invasion of their privacy, thinking that the personal password that is used to access their messages precludes anyone else from reading them.[12] Many e-mail systems, however, automatically copy messages to a back-up system,[13] where an employer can read them even if the employee deleted the message from his or her own personal computer.[14] Currently, many employers do not have written policies regarding the monitoring of e-mail, further compounding the lack of employee knowledge as to the extent of the intrusion.[15]

Moreover, the invasions of employees' privacy may not stop once their supervisor accesses and reads their e-mail. Disclosure of the contents of the e-mail messages to third parties may be even more harmful and invasive. Consider the following scenario:

Hypothetical One

An employee has filed an Equal Opportunity Claim against his company. In an attempt to air frustrations and educate others, both within the company and outside of it, the employee has sent out various e-mail messages describing the alleged violations, often describing the anger and frustration he has experienced. The supervisor, who fears the trouble the employee may cause, decides to copy all of the employee's e-mail messages and send them to a psychologist, without the employee's knowledge. The supervisor wants the psychologist to declare the employee a danger to the office, due to the anger expressed in the messages, and place the employee on leave.

In this case, the employee's privacy is further invaded by disclosing the contents of e-mail messages, which may be personal or business related, to an outside party.[16]

---

manipulate private information); Lee, *supra* note 4, at 144 (citing fears of voyeurism and employer paranoia as examples); Wilborn, *supra*, note 8, at 834-35 (discussing employees' fundamental interest in privacy); Flanagan, *supra* note 8, at 1262.

[12] *See* Gantt, *supra* note 11, at 349-50; Lee, *supra* note 4, at 145; Note, *supra* note 5, at 1909-10.

[13] "Back-up" is the copying of files to a secondary computer system in case the primary system fails, so no information is lost. *See Backup*, WHATIS, Sept. 29, 1999, *available at* <http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,211633,00.html>. This is usually a routine process that may be done automatically. *See id.*

[14] *See* Lee, *supra* note 4, at 141; C. Forbes Sargeant, III, *Electronic Media and the Workplace: Confidentiality, Privacy and Other Issues*, BOSTON B.J., May-June 1997, at 6, 6; Myrna L. Wigod, *Privacy in Public and Private E-Mail and On-Line Systems*, 19 PACE L. REV. 95, 108 (1998); Michael W. Droke, Comment, *Private, Legislative and Judicial Options for Clarification of Employee Rights to the Contents of Their Electronic Mail Systems*, 32 SANTA CLARA L. REV. 167, 170 (1992); Lehman, *supra* note 9, at 99.

[15] *See* Gantt, *supra* note 11, at 347.

[16] *See* Anderson Consulting LLP v. UOP, 991 F. Supp 1041, 1042 (N.D. Ill. 1998)

Employees who look to the law to address concerns over invasion of their privacy as a result of e-mail monitoring have found that it is not only ambiguous in its application to e-mail monitoring and disclosure, but also favors employers' interests.[17] Federal and state constitutional safeguards are inapplicable to employees in the private sector.[18] The controlling federal statute, the Electronic Communications Privacy Act of 1986 ("ECPA"),[19] fails to adequately protect private sector employee interests in e-mail privacy.[20] The ECPA distinguishes between messages that are intercepted while in transmission and those that are copied from storage, giving differing levels of privacy protection depending on the status of the message.[21] This distinction ignores the instantaneous transmission of e-mail that renders Title I protections against interception, as currently applied, virtually inapplicable to e-mail.[22]

(involving e-mails sent by Anderson employees while performing work for UOP which were released to the *Wall Street Journal* and used in a damaging story about Anderson).

[17] *See* Lee, *supra* note 4, at 151 (noting the ambiguities and exceptions within the law that support employer monitoring); Note, *supra* note 5, at 1910 ("The novelty of electronic mail corresponds to the paucity of legal precedents establishing the amount of privacy that protects its use."); Alexander I. Rodriguez, Comment, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439, 1441 (1998).

[18] *See* Wigod, *supra* note 14, at 110 (noting that constitutional protections are limited by the requirement of state action); Flanagan, *supra* note 8, at 1264-65 (stating that the protection of the Fourth Amendment of the U.S. Constitution applies only to public employees, and that most state constitutional provisions do not exceed this level of protection). Of the states that provide additional protection, only California courts have held that their state constitutional right to privacy extends to private employers. *See* Flanagan, *supra* note 8, at 1265. In California, an employee must have a reasonable expectation of privacy, and the employer must demonstrate a compelling interest. *See id.* at 1265-66.

[19] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.). The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") to bring electronic communications within the reach of the statute. S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N 3555, 3555. The ECPA is the only federal statute that governs the access and interception of electronic communications. *See* Gantt, *supra* note 11, at 351; Wigod, *supra* note 14, at 113.

[20] *See* Flanagan, *supra* note 8, at 1269-70 (explaining that employers have virtually unrestricted freedom to monitor employee communications under the ECPA regime); Note, *supra* note 5, at 1911. The ECPA provides employers with a number of statutory exceptions that in effect allow limitless monitoring and disclosure of employee e-mail. *See* Flanagan, *supra* note 8, at 1269; s*ee also infra* Section III-B.

[21] *See* 18 U.S.C. §§ 2511(1), 2701(a) (1994 & Supp. IV 1999); Greenberg, *supra* note 8, at 247-49 (noting the irrationality of the different protections offered under Title I and Title II of the ECPA).

[22] *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460-61 (5th Cir. 1994) (holding that the seizure of unread e-mail residing on a host computer was not an "intercept" as required by Title I, which contemplates an "intercept" of electronic

Therefore, employees are only left with Title II protections for stored messages, which are subject to an even broader exception than those under Title I, resulting in less employer liability for interception and disclosure.[23] Furthermore, Title II provides for a lesser damage award for violation as compared to Title I.[24] While many states have statutes that provide protection beyond that of the ECPA, including protection against invasions of privacy in the private sector workplace, these laws are often inapplicable due to the interstate nature of e-mail, which easily travels across state boundaries outside of the reach of the statute.[25]

III. E-MAIL PRIVACY PROTECTIONS UNDER THE ECPA.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[26] together with the 1986 ECPA amendment, is known as the Federal Wiretap Statute.[27] Title III was a legislative enactment designed to comport with the Supreme Court's holding in *Katz v. United States* that warrantless wiretapping is a Fourth Amendment violation.[28] Title III was intended to protect the security and privacy of personal and business communications.[29] The statute prohibited "aural interceptions"[30] of wire or oral communications by private individuals and government officials without a warrant.[31] Interception of a

communications as occurring during transmission); Wesley College v. Pitts, 974 F. Supp 375, 385 (D. Del. 1997) (finding that an "intercept" under Title I does not include the resulting storage of an e-mail message); White, *supra* note 9, at 1083 (noting that under current interpretations, it is "virtually impossible" to apply Title I protections to e-mail); *see also supra* note 1 and accompanying text.

[23] *See Wesley*, 974 F. Supp at 389 (noting that the court is troubled by the gap in coverage between Title I and Title II); *infra* Section III-B-1.

[24] *See* 18 U.S.C. § 2520(a)-(c) (providing for recovery of actual damages, profits made by violator as a result of the violation, punitive damages, and statutory damages for Title I Violations); *id.* § 2707(a)-(c) (providing only recovery for actual damages and profits made by violator as a result of the violation for Title II violations).

[25] *See* Lee, *supra* note 4, at 170.

[26] *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801-04, 82 Stat. 197, 211-25 (codified at 18 U.S.C. §§ 2510-20); *see also* Greenberg, *supra* note 8, at 223-24.

[27] *See* Greenberg, *supra* note 8, at 223-24.

[28] 389 U.S. 347, 353 (1967); *see also* Greenberg, *supra* note 8, at 225 & n.21.

[29] *See* Greenberg, *supra* note 8, at 225-26.

[30] "Aural transfers" contain the human voice at any point during the communication. *See* ECPA, 18 U.S.C. § 2510 (18) (1994). Therefore an "aural interception" would involve listening in on the conversation of another, whether it occurs from another room (oral interception) or over a phone line (wire interception). Electronic communications, on the other hand, do not involve transfers of the human voice, and therefore received no protection under Title III. *See* Greenberg, *supra* note 8, at 227, 232.

[31] *See* 18 U.S.C. § 2511(1) (1982); Greenberg, *supra* note 8, at 227-28.

communication under a court ordered warrant was not within the protection of the Wiretap Statute.[32]

However, courts had problems interpreting the amount of protection offered to private sector employees due to the ambiguous language of the statute.[33] An initial problem encountered by the courts in interpreting Title III was how to construe the meaning of "intercept."[34] The statute provided that an "interception" occurred only when an aural acquisition was made through the use of "any electronic, mechanical, or other device."[35] Federal courts debated whether a telephone extension provided by a common carrier was an "interception device" subject to the provisions of the statute.[36]

Title III had other limitations in addition to this ambiguity. By relying on aural interceptions, Title III was rendered inapplicable to many modern communication technologies that do not rely on the transmission of the human voice.[37] For example, Title III failed to apply to many new forms of communication such as voice mail, e-mail, and cellular phones in which the message involves the transmission of digital information.[38] A further limitation in Title III was its restriction to interceptions of telephone or wire communications provided by a common carrier, thereby excluding private communication systems from any form of privacy protection.[39] By 1985 Title III was "hopelessly out of date," and in drastic need of amendment.[40]

The ECPA, passed in 1986, was intended to amend and "clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[41] A key feature was the addition of "electronic communication" to clauses that previously covered only wire or oral communications.[42] While e-mail is not specifically addressed in the

---

[32] *See* 18 U.S.C. §§ 2516-18 (1982).

[33] *See* Greenberg, *supra* note 8, at 228-31.

[34] *See id.*

[35] 18 U.S.C. § 2510(4) (1982).

[36] *See* Greenberg, *supra* note 8, at 228-31 (discussing the various interpretations of interception under pre-ECPA Title III); *compare* United States v. Christman, 375 F. Supp. 1354, 1355 (N.D. Cal. 1974) (finding that an extension telephone is not an intercepting device), *with* Campiti v. Walonis, 611 F.2d 387, 391-92 (1st Cir. 1979) (rejecting the extension telephone exception and declaring that the nature of the equipment is not a part of the inquiry), *and* United States v. Harpel, 493 F.2d 346, 351-52 (10th Cir. 1974) (rejecting the *Christman* rationale and finding monitoring with an extension telephone a violation of Title III).

[37] *See* Greenberg, *supra* note 8, at 227, 231-32.

[38] *See id.* at 231-32 & n.63; Winters, *supra* note 4, at 117.

[39] *See Christman*, 375 F. Supp. at 1355.

[40] S. REP. NO. 99-451, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

[41] *Id.* at 1, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555..

[42] *See id.* at 14, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556, 3568; Greenberg, *supra*

statute, the legislative history notes that e-mail is to be given privacy protection under the ECPA as a form of electronic communication.[43] As a result of the addition of electronic communications to the protection of Title III, interceptions are no longer restricted to those involving the human voice, but now include "aural *or other acquisition* of the contents of any wire, electronic, or oral communication . . . ."[44] The ECPA also removed the common carrier restriction, thus bringing private telephone networks within the protection of the ECPA.[45] In addition to redefining "interception" and bringing private networks within the reach of the statute, Congress expanded the interception device requirement to include devices that intercept electronic communications.[46] This was accomplished by requiring only that the communications service provider furnish the device and use it in the ordinary course of business.[47] It was previously required that the device be furnished by a common carrier.[48] Finally, the ECPA added a new section, Title II, covering "stored communications" which applies to communications that are stored on a computer.[49]

A. *E-mail Protection Under Title I and Title II of the ECPA.*

Title I of the ECPA prohibits the interception and disclosure of wire, oral or electronic communications.[50] The state of mind required for an unlawful interception under the statute is "knowledge" that there was an intentional interception or "reason to know" that the information had been illegally intercepted.[51] The state of mind requirement ensures that inadvertent interception is not an ECPA violation.[52] Title I prohibits the government, employers, and third parties from intercepting the contents of messages.[53] However, the current interpretation of "intercept" as applied to e-mail leaves

note 8, at 232-33; Winters, *supra* note 4, at 117.

[43] *See* S. REP. NO. 99-451, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

[44] ECPA, 18 U.S.C. § 2510(4) (1994) (emphasis added).

[45] *See* S. REP. NO. 99-451, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556-57 (noting that many communications services are no longer limited to common carriers after the deregulation of the telecommunications industry).

[46] *See* 18 U.S.C. § 2510(5) (1994); Greenberg, *supra* note 8, at 235-36 (discussing the "extension telephone" exception); Winters, *supra* note 4, at 117.

[47] *See* 18 U.S.C. § 2510(5)(a).

[48] *See* 18 U.S.C. § 2510(5)(a)(i) (1982).

[49] *See* 18 U.S.C. §§ 2701-11 (1994).

[50] *See id.* at § 2511(1).

[51] *See id*.

[52] *See* S. REP. NO. 99-541, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3560.

[53] *See* 18 U.S.C. § 2510(8) (defining "contents" to include only the substance or meaning of the communication); *id.* § 2511(1); Gantt, *supra* note 11, at 352; Wigod, *supra* note 14, at 113.

only a small window of opportunity in which the interception may come within Title I of the ECPA. Once a message has been sent and routed to the recipient's e-mail box, the transmission has ceased and the message is subject only to the Title II protections for stored messages.[54] An interception under Title I may still occur when a message is copied while in transmission before it has been properly routed to the recipient's mailbox.[55] It is important to note that the ECPA only protects the contents of messages, leaving employers free to monitor the transactional information of the e-mail, including who the sender and recipient are, the length of the message, and e-mail subject headings.[56]

Few courts have analyzed the legality of intercepting e-mail messages under Title I, and these have usually found liability under the Title II provision for stored messages instead.[57] Much of the analysis of e-mail under the ECPA has attempted to prove the occurrence of a Title I interception.[58] This is because Title I provides greater protections due to more restrictive exceptions than Title II.[59] Additionally, Title II does not punish disclosure of an intercepted stored message.[60] Most importantly, Title I provides for actual damages and profits as well as both statutory and punitive damages unlike Title II which limits damages to actual damage or profit.[61]

The difficulty in proving a Title I interception of e-mail is the satisfaction of the statutory requirement of an "intercept." For example, the court in *Wesley College v. Pitts* noted that the ECPA requires that a "device" be used in the interception under Title I.[62] Furthermore, *in Steve Jackson Games, Inc. v. United States Secret Service* the court noted that interception must occur

[54] *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460-62 (5th Cir. 1994) (holding that the seizure of unread e-mail residing on a host computer was not an "intercept" as required by Title I, which contemplates an "intercept" of electronic communications as occurring during transmission); Wesley College v. Pitts, 974 F. Supp 375, 385-86 (D. Del. 1997) (finding that an "intercept" under Title I does not include the resulting storage of an e-mail message); White, *supra* note 9, at 1083 (noting that under current interpretations, it is "virtually impossible" to apply Title I protections to e-mail).

[55] See *supra* notes 13-15 and accompanying text.

[56] *See* 18 U.S.C. § 2510(8); *id.* § 2511; Wigod, *supra* note 14, at 113.

[57] *See, e.g.*, *Wesley College*, 974 F. Supp. at 381-89.

[58] *See, e.g.*, *Steve Jackson Games, Inc.*, 36 F.3d at 460-62; *Wesley College*, 974 F. Supp. at 381-89.

[59] *Compare* 18 U.S.C. § 2511(2), *with id.* § 2701(c).

[60] *See id.* § 2701(a).

[61] *See* 18 U.S.C. §§ 2520(b)-(c), 2707(b)-(c) (1994 & Supp. IV 1999).

[62] *See Wesley College*, 974 F. Supp. at 384 (finding that interception is a required component to a violation of Title I provisions against disclosure, and must comprise of more than accidental viewing of a message on the screen).

contemporaneously with the transmission for a Title I "interception" to occur.[63] The *Wesley* court further noted that a Title I "interception" cannot apply to electronic communications in storage according to the definitions of "intercept," "wire transmissions," and "electronic communications," thus affirming the *Steve Jackson Games* court's decision.[64] Moreover, there are a number of exceptions which may exempt employers from liability under Title I of the ECPA, allowing them to access and monitor employee e-mail.[65]

Title II of the ECPA governs stored communications.[66] This section imposes liability for a person who accesses stored messages without authorization, or exceeds authorization to access the information.[67] An e-mail message, once received and stored on the system is a "stored communication" subject only to Title II protections.[68] Title II will cover most monitoring, interception, and disclosure of e-mail because employers will likely view messages from a back-up copy or from the storage itself. However, like Title I, there are statutory exceptions allowing providers of communication services to access and disclose messages.[69] However, the Title II exception proves to be broader than those of Title I.

B. *Statutory Exceptions to Title I and Title II of the ECPA*

1. Provider Exception

There are four statutory exceptions to the ECPA: the system provider exception;[70] business use exception;[71] prior consent;[72] and the exception for

---

[63] *See Jackson Games, Inc.*, 36 F.3d at 460-62 (finding no intercept, as required for a Title I violation, when agents seized a computer with stored, but unread, messages on it).

[64] 974 F. Supp. at 385-86 (noting that unlike "wire communications", the definition of "electronic communications" does not include electronic storage of such communications).

[65] *See* 18 U.S.C. § 2511(2)(a)(i) (allowing providers of an electronic communications service to intercept, disclose or use that communication in the normal course of employment if necessary to render service or protect property); *id.* at § 2511(2)(d) (allowing interception, use or disclosure if one of the parties has given prior consent); § 2510(5)(a) (exempting interceptions made by devices used in the ordinary course of business); *see also infra* Section III-B-1 to -4.

[66] *See* 18 U.S.C. § 2701(a). The ECPA defines stored electronic communications as those in "any temporary, intermediate storage . . . incidental to the transmission . . ." as well as "any storage . . . by an electronic communication service for purposes of backup protection . . ." 18 U.S.C. § 2510 (17).

[67] *See* 18 U.S.C. § 2701(a).

[68] *See id.*; Wigod, *supra* note 14, at 116. However, as one commentator points out, e-mail messages may be technically stored at many points. *See id.*

[69] *See* 18 U.S.C. § 2701(c)(1).

[70] *See id.* §§ 2511(2)(a)(i), 2701(c)(1), 2702(b)(5).

[71] *See id.* § 2510(4), (5)(a).

communications that do not affect interstate commerce.[73] The primary exception that applies in the context of e-mail monitoring is the provider exception to the ECPA.[74] This exception exempts system providers from liability under Title I and Title II for interception, use, or disclosure.[75] The importance of this exception is grounded upon the fact that unless an employer automatically copies all incoming and outgoing messages within the meaning of "intercept" as defined by the courts, the interception of messages will occur while they are in storage. This exception thus appears to give the employer broad license to monitor, intercept, and disclose messages in any form as long as they provide the service.[76] In order to qualify for this exemption under Title I, an employer must be a system provider and intercept, use, or disclose the message within the ordinary course of business while performing activities necessary to render the communications service or protect property.[77] The provider exception for Title II is much broader, requiring only that the employer qualify as a service provider.[78]

The statutory definition of a service provider refers to "facilities for the transmission of electronic communications and any computer facilities or electronic equipment for the electronic storage of such communications . . ."[79] and "any service which provides users thereof the ability to send or receive wire or electronic communications . . . ."[80] While this language may not clarify whether a private employer who provides e-mail only to its employees is a "provider,"[81] some commentators believe that an employer providing this type of service would fall under the ECPA exception.[82] One commentator has argued that the term "service" implies an external service provider with the

[72] *See id.* § 2511(2)(d), 2702(b)(3).

[73] *See id.* § 2510(12).

[74] *See id.* §§ 2511(2)(a)(i), 2701(c)(1), 2702(b)(5).

[75] *See* 18 U.S.C. §§ 2511(2)(a)(i), 2701(c)(1), 2702(b); s*ee also* White, *supra* note 9, at 1088.

[76] *See infra* Section IV (discussing issues and exceptions regarding disclosure of intercepted messages).

[77] *See* 18 U.S.C. § 2511(2)(a)(i).

[78] *See id.* § 2701(c)(1).

[79] *Id.* § 2510(14).

[80] *Id.* § 2510(15).

[81] *See* White, *supra* note 9, at 1088-89 (doubting whether a private employer who offers e-mail to its employees would be characterized as a provider).

[82] *See* Lee, *supra* note 4, at 156 (stating that companies with their own e-mail networks could fall under the system provider exception); Greenberg, *supra* note 8, at 236-37 (noting that the inclusion of private communication networks within the scope of the ECPA supports the inclusion of an employer providing e-mail to its employees within the system provider exception).

company as the "user," therefore not within the act as a "provider."[83] If an employer provides e-mail service through an outside provider, then they may not fall under the provider exception.[84] What arguably emerges from the Title II exception is a "basic rule for stored communications that there are virtually no protections or restrictions on . . . employers regarding access."[85] Employers intercepting mail under Title I may not have such a broad exemption to monitor all mail, but this remains to be tested in the courts.[86] Taken together, the Title I and Title II provider exceptions will exempt most private companies from liability for monitoring or disclosing communications occurring on its system.[87]

2. Ordinary Course of Business Exception

The second applicable exception is the ordinary course of business exception, which arises only under Title I, and governs the interception of communications.[88] This exception allows a service provider to intercept, use, or disclose a communication if the interception involved telephone equipment or facilities used within the ordinary course of business.[89] Though Title I sees little application to e-mail as currently applied, judicial interpretation of "intercept" as well as technological advances make future application of Title I to e-mail more likely.[90] While, this exception has not yet been applied in the context of e-mail, much interpretation has been done in the context of telephone monitoring.[91] Judicial interpretation of the "ordinary course of business" language has resulted in two divergent approaches, the "context" and "content" approaches.[92] The context approach evaluates the monitoring from the perspective of the employer, looking at the circumstances of the workplace and any employee expectations of privacy. [93] The content approach evaluates

[83] *See* Droke, *supra* note 14, at 182.

[84] *See* Gantt, *supra* note 11, at 360.

[85] Wigod, *supra* note 14, at 116.

[86] *See* Gantt, *supra* note 11, at 359-64 (cautioning that pre-ECPA telephone monitoring cases and legislative history suggest that employers may not have unrestricted access to monitor e-mail and read the contents of messages); s*ee also supra* Section III-A (discussing the limitations of "intercept" under Title I).

[87] *See* Gantt, *supra* note 11, at 359.

[88] *See* ECPA, 18 U.S.C. § 2510(5)(a) (1994).

[89] *See id.* § 2510(4), (5)(a). This is because the definition of an intercepting device required for Title I specifically excludes telephone and telegraph devices and facilities used in the ordinary course of business. *See* Gantt, *supra* note 11, at 364.

[90] *See supra* notes 20-24 and accompanying text; *supra* Section III-A.

[91] *See* Gantt, *supra* note 11, at 364-65; Wigod, *supra* note 14, at 114-16.

[92] *See* Gantt, *supra* note 11, at 364-73 (discussing the content versus context approaches applied by courts to telephone monitoring cases and possible applications to e-mail).

[93] *See id.* at 365-67.

the monitoring by looking at the content of the message, whether it is business related or personal, and whether the business has any interest in that content.[94]

a. *Context Approach*

In applying the context approach, the court looks at the business justifications for monitoring and whether employees had any notification of monitoring.[95] One commentator sees this approach as judging the interception according to the employee's expectation of privacy, although the ECPA has no such requirement.[96] The Eighth Circuit has divided the test under this approach into two separate questions, the first asking whether the device was provided by the communications service provider or connected to a phone line, and the second inquiring if the interception was within the ordinary course of business.[97]

In the context of e-mail, the first inquiry would involve examining how the employer is connected to the Internet. Currently most users are connected through modems or networks that use phone lines. These devices seem to satisfy the Eighth Circuit's first question. It seems likely that a court applying the context approach would look less at the offending device and more at the second question, the situation surrounding the monitoring. The court could consider factors such as: the employment environment;[98] the type of system used;[99] or the existence of monitoring policies.[100] However, the inquiry tends to establish the reasonableness of the employee's expectation of privacy as well as reviewing the context of the work environment.

b. *Content Approach*

While the context approach focuses on the situation surrounding the interception, the content approach reasons that employers have an interest in calls that are business related, but not those that are personal.[101] *Watkins v.*

---

[94] *See id.* at 367-69.

[95] *See id.* at 365.

[96] *See id.*

[97] *See* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (finding that an employer who tape recorded twenty-two hours of calls, most of which were personal, did not qualify for the business extension exception).

[98] *See* Droke, *supra* note 14, at 185.

[99] *See id.* The type of system may be determined by how employees gain access, for example whether a password is required. *See id.* Further considerations as to the type of system may include factors such as the ability to designate messages as confidential, or separation of personal and business e-mail accounts. *See id.*

[100] *See id.* at 184-85.

[101] *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 582-84 (11th Cir. 1983); Gantt, *supra* note 11, at 367.

L.M. Berry & Co. was the first case where a court used a content approach.[102] This decision held that employers must show that the interception was in pursuit of a legal interest.[103] The court noted that monitoring personal calls is never in the ordinary course of business and the employer may only monitor to determine if the call is personal or not, and if personal, must immediately cease monitoring.[104] Other courts have construed the employer's business interest more broadly to include personal conversations between employees about their supervisors.[105]

In applying these approaches to e-mail, courts using the context approach will look at whether employees were notified of possible monitoring and circumstantial factors in the workplace; courts applying the content approach would allow employers to intercept messages with business content, but not personal messages.[106] However, neither of these approaches sufficiently guarantees employee privacy because they assume that there is little or no independent right to privacy in communications.[107] Under the context approach, an employer may intercept messages as long as employees were notified and had little or no expectation of privacy.[108] Further compounding this issue is the lack of awareness employees may have regarding how e-mail works and the extent of employer monitoring.[109] Problems arise under the content approach as well, because employers still need to intercept and read e-mail in order to determine whether the message is business or personal. [110]

3. Prior Consent

The third exception to ECPA liability under both Title I and Title II is the prior consent exception.[111] Actual or implied consent may be sufficient to

---

[102] *See* Gantt, *supra* note 11, at 367.

[103] *See Watkins*, 704 F.2d at 582-83.

[104] *See id* at 583.

[105] *See* Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 416-17 (11th Cir. 1986) (finding that a call between employees during working hours in which there was personal discussion about supervisors implicates the employer's legal interests); Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (extending the employer's interest to allow for non-consensual monitoring of calls if limited to the business portion of the call).

[106] *See* Gantt, *supra* note 11, at 369-70.

[107] *See id.* at 370.

[108] *See id.*

[109] *See supra* text accompanying notes 12-15.

[110] *See* Gantt, *supra* note 11, at 370.

[111] *See* ECPA, 18 U.S.C. § 2511(2)(d) (1994) ("It shall not be unlawful . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent . . . ."); *id.* § 2702(b)(3) ("A person or entity may divulge the contents of a communication . . . with the lawful consent of the originator or an . . . intended recipient . . . .").

shield the employer from liability.[112] Although the consent exception has not been specifically addressed in the context of e-mail messages, courts have interpreted it under telephone monitoring cases.[113] The *Watkins* court addressed the consent exception, concluding that consent must be specific and limited, and generally should not be implied from the circumstances.[114] The court further noted that consent would be implied when the employee knew or should have known that constant monitoring may occur or when the employee has personal conversations on a phone line reserved for business purposes.[115] A more recent decision has reaffirmed the limited scope of the consent exception.[116] In *Deal v. Spears*, the court refused to find consent based only on the employer's warning that telephone monitoring may occur.[117] These court decisions, while limiting the consent to specific circumstances, suggest that an employer with a monitoring policy in place may escape liability for intercepting e-mail messages.[118]

4. Interstate Commerce Requirement

The final exception to the ECPA rests upon the statute's foundation as federal legislation passed by Congress under the authority of the commerce clause of the Constitution.[119] This requirement of the ECPA exempts employers whose communications do not affect interstate commerce from liability under Titles I and II. Systems that would be covered under this exception are limited to intrastate or intra-company networks. In the context of modern e-mail systems, this exception will apply to few employers.[120] There is a possibility that some purely intra-office e-mails may be sent. However, if they require the typical telephone/modem connection, the possibility of interstate transmissions of e-mail messages or the use of interstate communications systems increases, therefore implicating the ECPA.[121]

Together, these exceptions to the ECPA give an employer many opportunities to monitor an employee's e-mail with little fear of liability.[122]

---

[112] *See* Gantt, *supra* note 11, at 356.

[113] *See id.*

[114] Watkins v. L.M. Berry & Co., 704 F.2d 577, 581-82 (11th Cir. 1983).

[115] *See id.*

[116] *See* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992).

[117] *See id*.

[118] *See* Gantt, *supra* note 11, at 357-58.

[119] *See* ECPA, 18 U.S.C. § 2510(12) (1994) (defining an "electronic communication" as "any transfer . . . that affects interstate or foreign commerce").

[120] *See* Gantt, *supra* note 11, at 353-54 n.61 (noting the Supreme Court's broad interpretation of the meaning of interstate commerce and the likelihood that few privacy claims would be thwarted by this requirement).

[121] *See id.*

[122] *See id.* at 357-58; *supra* notes 70-121 and accompanying text.

For example, an employer that provides its employees with e-mail, thus qualifying as a provider, may intercept the messages without fear of ECPA liability under either Title I or II.[123] Moreover, in the event that Title I is applied to e-mail, the employer may escape liability by satisfying the business use exception, regardless of the approach used by the courts.[124] The employer may qualify under the context approach by publishing a monitoring policy and notifying employees that it will ensure compliance with e-mail policies through monitoring.[125] The employer may satisfy the content approach by intercepting only those messages with business content, or those related to broadly construed business interests.[126] Finally, an employer may escape liability by establishing employee consent to monitoring.[127] This may easily be accomplished through the use of monitoring policies and implied consent from continued use of the e-mail system accompanied by knowledge that monitoring will occur.[128]

IV. THE PROBLEM OF DISCLOSURE TO THIRD PARTIES

While current law provides employers with many ways to monitor employee e-mail usage without incurring ECPA liability, a further, unaddressed question arises. Once an employer has lawfully intercepted a message, what controls the use of information contained therein? The ECPA has provisions against use and disclosure of information gathered from an illegally intercepted message.[129] However, given the variety of exceptions available to employers that exempt them from liability for intercepting a message, employees still lack any protection or certainty. This section will examine the current ECPA provisions regarding disclosure of messages and how they may apply to e-mail in the private sector workplace.

Hypothetical One, discussed in the beginning of this note, reflects the use of intercepted e-mail against the employee.[130] Employees without protection who send personal messages risk that their employers may intercept the message and use it against them. For example, a message including scandalous remarks about a supervisor may be intercepted and disclosed to those who make promotional decisions, or discussed with a future employer during a check on references.[131] Another example of an intercepted message disclosed to the

[123] *See supra* Section III-B-1.

[124] *See supra* Section III-B-2.

[125] *See supra* Section III-B-2-a.

[126] *See supra* Section III-B-2-b.

[127] *See supra* Section III-B-3.

[128] *See supra* Section III-B-3.

[129] *See* ECPA, 18 U.S.C. §§ 2511(1)(c), 2702(a) (1994); *see also supra* Section III-A.

[130] *See supra* Section II.

[131] A court using a broadly construed content approach to the ordinary course of business

detriment of the sender could involve the interception of a message discussing a medical situation. The employer may then disclose that information to its insurance carrier to determine the cost of the medical treatment and its effect on the employer's insurance costs. If the employee requires expensive medical care, the employer may then discharge the employee to avoid paying the increased insurance premium. However, not all disclosures may reflect the malignant heart of the employer.

A message may be disclosed for reasons not related to the continued employment of the employee. For example, imagine the following situation:

Hypothetical Two

An employee has recently been raped. She sends an e-mail message from work to a friend discussing the assault and her resulting mental distress. The employer, in the course of monitoring, reads the e-mail and feels genuine concern for the employee. The supervisor discloses the information to a company therapist, or an outside therapist, wondering what can be done to help the employee through her ordeal.

In this situation, the employer only has the best interests of his or her employee in mind, yet the disclosure involves an invasion of the employee's privacy and dissemination of highly personal information. Disclosure to third parties may have consequences outside of the employment context.

In one of the few cases discussing the specific issue of disclosure, *Anderson Consulting LLP v. UOP*, the e-mails sent by Anderson Consulting while it was doing a job were later disclosed to a newspaper and became the subject of a damaging story.[132] Anderson looked to the ECPA for protection, relying on Title II protection against the disclosure of stored communications.[133] Both Titles I and II of the ECPA prohibit disclosure of the contents of intercepted and stored messages respectively.[134] However, the broad exceptions available to employers result in little applicability of the ECPA to disclosure by a private sector employer.[135]

A. *Disclosure Under Title I*

Title I of the ECPA states that one who "intentionally discloses, or endeavors to disclose to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication

exception would see no problem with this interception, because of the employer's interest in employee/supervisor relations. *See supra* Part III-B-2-b.

[132] 991 F. Supp. 1041, 1042 (N.D. Ill. 1998).

[133] *See id.* at 1042; s*ee also* 18 U.S.C. § 2702(a)(1).

[134] *See* 18 U.S.C. §§ 2511(1)(c), 2702(a).

[135] *See supra* Section III-B.

[violates] this subsection . . . ."[136] To trigger liability under this section, an employer must "intercept," "disclose," and fail to qualify for any exception. An intercept can occur through the use of any "electronic, mechanical or other device or apparatus which can be used to intercept a[n] . . . electronic communication . . . ."[137]

In the context of e-mail, there is a limited time period in which an e-mail is being transmitted, before it becomes a stored communication subject to Title II.[138] Therefore, the employer must intercept within this time period while the message is in transit in order to be liable under Title I.[139] Furthermore, the interception must be a result of affirmative action on the part of the employer.[140] The technology involved in e-mail has been misunderstood. As e-mail is sent it is often automatically copied without any action required by the user.[141] Likewise, there is no affirmative action necessary for the interception to occur, it happens automatically due to the program and back-up requirements.[142] This distinction has yet to be recognized by the courts in interpreting e-mail interception under the ECPA. In the context of *Hypothetical One*, the employer accessed the messages after they had been sent.[143] Under current judicial analysis, the messages would be subject only to Title II protections.[144]

The second barrier to liability requires that the employer who discloses must know or have reason to know that the interception was a violation of the ECPA.[145] Therefore, even an intentional disclosure will not subject an employer to liability if there was no reason to know that it was a violation of the ECPA. Both of these elements, interception and disclosure, must be present for liability under Title I.[146]

Finally, in order to be liable for a disclosure under Title I, the employer must not qualify for any of the broad exceptions.[147] Given the number of exceptions and the difficulty of "intercepting" a message, employers may rarely find themselves in a situation where they will be violating the statute.

---

[136] 18 U.S.C. § 2511(1)(c).

[137] *Id.* §§ 2510(4), (5).

[138] *See supra* text accompanying notes 54-61.

[139] *See* Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del. 1997).

[140] *See id.* at 381.

[141] *See supra* text accompanying notes 12-15.

[142] *See supra* text accompanying notes 12-15.

[143] *See supra* Section II.

[144] *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994); Anderson Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998); *Wesley*, 974 F. Supp. at 389.

[145] *See* 18 U.S.C. § 2511(1)(c) (1994).

[146] *See Wesley*, 974 F. Supp. at 383-84.

[147] *See supra* Sections III-B-1 to -4.

There needs to be legislative and judicial revision of the concepts involved in e-mail interception in order to restrain employers' monitoring activities.

Furthermore, the ECPA is silent as to whom lawfully intercepted information may be disclosed. Courts that have addressed disclosure issues have never resolved this issue.[148] Until the courts resolve a case or legislative clarification occurs, employees face uncertainty as to the extent of the travels of their personal information gathered from intercepted e-mail messages.

B. *Disclosure Under Title II*

Title II of the ECPA, unfortunately, offers employees even less protection from disclosure of their e-mail messages than Title I. Title II applies to e-mail messages that are classified as stored communications.[149] Title II prohibitions on disclosure only require that "a person or entity providing an electronic communication service *to the public* shall not *knowingly* divulge . . . the contents of a communication while in electronic storage . . . ."[150] Title II therefore allows disclosure of stored communications if the disclosing party is not a public provider. Thus, an employer providing e-mail to its employees "can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage."[151]

In *Anderson*, the plaintiff argued that UOP should be liable under Title II prohibitions on disclosure.[152] In interpreting the word "public," the court, in the absence of a statutory definition, declared the word unambiguous and applied it to mean the community at large, not simply employees.[153] The court refused to consider Anderson's argument that the legislative history suggested that an employer who provides e-mail to employees should be liable under the act.[154] The court stated that since "public" is unambiguous, there was no need to consider the legislative history.[155] The court noted that providing a system to communicate with "personnel, third party vendors, and other third parties

---

[148] *See Anderson*, 991 F. Supp. at 1042-43 (resolving the case on other issues and never discussing the limits of disclosure); *Wesley*, 974 F. Supp. at 383 (failing to discuss the disclosure of intercepted information to a spouse and children).

[149] *See supra* notes 66-69 and accompanying text.

[150] 18 U.S.C. § 2702(a)(1) (emphasis added); s*ee also* Muskovich v. Crowell, No. CIV. 3-95-CV-20007, 1996 WL 707008, at *4-*5 (S.D. Iowa Aug. 30, 1996) (finding that "knowledge" under section 2702 is more than knowledge of a possibility, and requires a substantial certainty that disclosure will occur).

[151] *Wesley*, 974 F. Supp at 389 (agreeing that this disparity in treatment is troubling, but must be corrected through legislative action).

[152] *See Anderson*, 991 F. Supp at 1042.

[153] *See id.* at 1042-43.

[154] *See id.* at 1043.

[155] *See id.*

both in and outside of Illinois" was not a public service.[156] Given the difficulty in classifying employers as public providers, it would appear that the employers involved in *Hypothetical One*[157] and *Two*,[158] if construed as Title II violators, would have no limits on their disclosures, leaving an employer free to discuss employee communications with whomever the employer encounters.

However, even if the employer could qualify as a public provider, there is a statutory exception allowing disclosure if necessary to protect the rights or property of the provider.[159] This exception may prove to be one of the few actual protections that employees have against disclosure in the unlikely event that an employer would be a "public" service provider. An employer would have difficulty arguing that content of employee e-mail, especially if not directly related to the business, is its property. Further, an employer would need to show that the disclosure was in protection of its property or interests. In the context of telephone monitoring, employee morale or productivity has served as a valid interest.[160] Applied to e-mail, the employer could possibly argue that the disclosure was necessary to improve morale or working conditions. However, the argument that personal information in employee e-mail messages is related to a business interest seems unlikely to succeed.

Titles I and II of ECPA thus provide little protection to employees not only against monitoring of their e-mail, but also against disclosure to other persons. The exceptions available for service providers give too much latitude to employers to violate employee privacy interests. Furthermore, the statute fails to restrict disclosure to parties with a valid interest. The legislative history is silent about to whom a properly intercepted message may be disclosed. With the number of businesses using e-mail on the rise, employees need further protection.

V. PROPOSALS TO PROTECT EMPLOYEE PRIVACY

Due to the inadequacies of current federal law, employers may engage in violating invasions and disclosures. Therefore, there needs to be clarification of the rights and responsibilities of both employees and employers.[161] Changes may occur in three different areas: employer e-mail policies, judicial interpretation of current law, and statutory reform. While e-mail policies may provide immediate clarification of e-mail rights in the workplace, they will primarily serve employer interests and fail to protect employee e-mail from intrusive interception and disclosure. Recognizing employee e-mail privacy

---

156 *Id.*

157 *See supra* Section II.

158 *See supra* Section IV.

159 *See* ECPA, 18 U.S.C. § 2702(b)(5) (1994).

160 *See supra* notes 101-05 and accompanying text.

161 *See* Flanagan, *supra* note 8, at 1271.

rights and balancing them against valid employer concerns will have to come from judicial interpretation of current law and new legislation. Of these two options, legislation is the best course of action to remedy defects, ambiguities, and gaps in current e-mail protection and provide continuing coverage for technological advances in the future.[162]

A. *Employer Monitoring Policies*

Employers have an incentive to establish e-mail policies not only to avoid employee misuse of the system, but also to reduce the possibility of liability.[163] Employers without policies face liability on two different fronts. First, employee misuse of e-mail systems may subject the employer to legal action for any wrongs committed by employees.[164] Second, lack of a policy regarding monitoring and disclosure of e-mail contents may subject the employer to legal actions by employees for invasion of privacy.[165] A detailed e-mail policy will reduce employer liability by informing employees of the expected level of privacy in their e-mail usage and ensuring employees that illegal e-mail activity will be caught.[166] A policy that specifies how, when, and why monitoring will occur and to whom the contents of the message may be disclosed will also assist courts in determining the reasonableness of the company's actions when a statute is ambiguous.[167]

A clear, detailed policy is necessary to alert employees to the monitoring and disclosure practices of the company and to deter misuse.[168] A policy that explains the employer's rationale for monitoring will also serve to reduce employee concerns over "eavesdropping" by the employer.[169] Notice of monitoring and the extent of disclosure to third parties warns the employees that continued usage of the e-mail system may result in an implied consent to the policy and a reduction of their e-mail privacy.[170] Employers may go further to state this explicitly and require employees to sign a waiver or have a

---

[162] *See id.*

[163] *See* Lee, *supra* note 4, at 173; Greenberg, *supra* note 8, at 249-50 (suggesting policies that would limit employee misuse of e-mail systems); Lehman, *supra* note 9, at 112 (explaining that an e-mail policy may limit liability for wrongs committed by employees through e-mail); White, *supra* note 9, at 1102-03 (noting that employers without e-mail policies risk liability for employee wrongdoing through the e-mail).

[164] *See* Lehman, *supra* note 9, at 109-10; White, *supra* note 9, at 1102 -03.

[165] *See* Gantt, *supra* note 11, at 405 (noting that existence of an e-mail policy is a strong defense to any employee claim of privacy invasion); White, *supra* note 9, at 1102.

[166] *See* Lee, *supra* note 4, at 173; Greenberg, *supra* note 8, at 249-50; Lehman, *supra* note 9, at 112; White, *supra* note 9, at 1102-03.

[167] *See* Lee, *supra* note 4, at 173.

[168] *See* Note, *supra* note 5, at 1913; White, *supra* note 9, at 1103.

[169] *See* Greenberg, *supra* note 8, at 250.

[170] *See* White, *supra* note 9, at 1103.

warning appear upon the computer screen after logging in to the e-mail system.[171] An explicit, conspicuous policy will also decrease the possibility that employees will misunderstand their privacy expectations, purpose of passwords, or the operation of the system.[172] Notice and consent, either express or implied, may give contractual rights to the employer, for example by stating that all messages sent through the company system are the property of the employer.[173]

Most importantly, every policy should state who will have access to the messages, for what purposes an intercepted e-mail may be used, and to whom the information may be disclosed.[174] This "disclosure policy" will ensure that employees are aware of the extent to which information contained in intercepted e-mail will be shared and discussed with others within the company and with third parties. For example, employee awareness that information contained in e-mail may be used against them in disciplinary actions or disclosed to future employers may result in employees tailoring their e-mail correspondence to that which is appropriate in the workplace.

In *Hypothetical Two*,[175] if there had been a policy alerting the employee that supervisors may monitor messages and discuss information contained therein with third parties, the employee may not have discussed a recent rape if she did not want the information to be disseminated at the employer's whim. If the policy stated, however, that personal information gathered during monitoring would never be disclosed, then the employee may continue to feel comfortable e-mailing confidential personal information from the company system. A "disclosure policy" will also serve to constrain the employer's actions, ensuring that they do not subject themselves to liability for invasion of privacy for disclosing the contents of an e-mail message to a third party.[176]

A reasonable "disclosure policy" should address the concerns of both the employer and the employee.[177] Employers have an interest in the contents of e-mail that are business-related.[178] The company would want to be able to

---

[171] *See* Droke, *supra* note 14, at 187-88; White, *supra* note 9, at 1103-04.

[172] *See supra* notes 12–15 and accompanying text; s*ee also* Lee, *supra* note 4, at 174.

[173] *See* Greenberg, *supra* note 8, at 250 (suggesting that monitored messages be treated as company records); White, *supra* note 9, at 1103 (noting that the e-mail system is the property of the company).

[174] *See* Lee, *supra* note 4, at 173; Droke, *supra* note 14, at 188; Greenberg, *supra* note 8, at 250.

[175] *See supra* Section II.

[176] *See supra* note 165 and accompanying text.

[177] *See* Greenberg, *supra* note 8, at 249-50 (stating that employers need to balance their business needs against the employees' privacy interests).

[178] *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 582-83 (11th Cir. 1983) (applying a content approach to the ordinary course of business exception and noting that employers have a legal interest in business communications, but never in personal communications);

disclose business-related contents to parties outside the company that also share this business interest. For example, a business and one of its customers may have an interest in the contents of an employee message that discusses a rival business. The employee's concern is disclosure of information contained in personal messages.

The employee and company may have conflicting beliefs as to who may have access to the information contained within an intercepted e-mail. It is possible that the employer may have a valid interest in disclosing the information from a personal message to persons within the company. For example, the company may wish to discuss an employee's personal e-mail comments about his or her boss's behaviors with the offending supervisor. However, for personal messages not related to employment, there should not be disclosure to persons within the company because it serves no valid business need and may only harm or embarrass the employee. Third parties should not have access to personal information contained within employee e-mail. This will not only protect employee e-mail privacy, but also offer protection to the employer. Information disclosed to a third party is out of the employers' control and may be disclosed to others, such as the media or rivals, with whom the employer did not want to share the information. This loss of control over the disclosed contents of the e-mail severely endangers the employee's privacy concerns and control over their personal e-mail messages.

A policy that limits e-mail use strictly to business purposes would avoid many issues that could arise from employees using e-mail for personal messages that may contain private and sensitive information.[179] Furthermore, a prohibition on monitoring of private e-mail within the workplace, or a complete disallowance of private e-mail, would further serve employee interests by reducing the possibility of the disclosure of personal information. The decision about allowance of private e-mail and its monitoring should be left to the employer, who is best able to judge his or her company's e-mail needs, limits, and employee concerns.[180]

It is important to note that while an e-mail policy explicitly warns employees of privacy invasions so they may alter their e-mail use accordingly, it does nothing to offer them protection.[181] While e-mail policies may be a step in the right direction to clarifying employee e-mail rights, they will lack the proper balancing of employee and employer interests that is offered through

Gantt, *supra* note 11, at 367; *see also supra* Section III-B-2-b (discussing the application of the content approach to e-mail).

[179] *See* Droke, *supra* note 14, at 187-88; Greenberg, *supra* note 8, at 250.

[180] *See* Lee, *supra* note 4, at 173 (explaining that an e-mail policy should be tailored to the work environment and needs of both employers and employees).

[181] *See* Gantt, *supra* note 11, at 405 (arguing that corporate e-mail policies primarily protect the interests of the employer and institutionalize new forms of monitoring and privacy invasion).

legal alternatives.[182] Finally, a floor of protection which the employer may not go below should be established either through interpretation of current law or passing of new legislation. This would ensure that employers do not attempt to contract away all employee privacy rights in the e-mail.

B. *Judicial Interpretation of Current Law*

Because employers draft the policies with their interests in mind, they fail to fully protect employee privacy interests.[183] In the event that a policy may not exist or is vague, employees and employers must turn to the law to address and balance the privacy interests of the employee against the employer's interest in monitoring conduct and performance.[184] However, current federal law regarding e-mail privacy and disclosure gives little assurance to either employers or employees.[185] In interpreting current law it is important for courts to establish a baseline of employee e-mail protection to ensure that employers respect a minimum amount of privacy in workplace communications. Short of new legislation, judicial interpretation of the ECPA in light of evolving communication technologies may serve as the best option to clarify and possibly expand employee interests in privacy of e-mail communications.[186]

Gaps exist between the emergence of new communication technology and the drafting of applicable statutes.[187] In this period courts may choose to allow new issues and causes of action under the old laws, thereby protecting users of new technologies from invasions of privacy.[188] It is argued that as this gap increases, courts should be more willing to accommodate plaintiffs, especially when a case turns upon a technicality in the statute that does not recognize the new technology.[189]

Foremost, the courts should reinterpret "intercept" under the Title I of the

---

[182] *See* Lee, *supra* note 4, at 173 (suggesting a flexible federal policy that balances employee and employer interests).

[183] *See* Gantt, *supra* note 11, at 405 (noting that e-mail policies will protect the employer, validate monitoring practices and compromise employee privacy). Gantt further warns that employees will most likely have no bargaining power over the terms of the policy and must accept them in order to continue employment. *See id.* at 407.

[184] *See* Greenberg, *supra* note 8, at 249.

[185] *See* Lee, *supra* note 4, at 139 (asserting that the laws addressing employee privacy rights with respect to e-mail are unclear).

[186] *See* Droke, *supra* note 14, at 192 (explaining that not all business will implement monitoring policies and the legal system must respond to ensure employees receive adequate protection).

[187] *See* Winters, *supra* note 4, at 130.

[188] *See id.*

[189] *See id*.

ECPA to more easily include e-mail.[190] A court could find that, considering how the technology and emerging interception software works, restricting "intercept" to such a minute period would thwart the goals of Congress. E-mail that is intercepted while in a form of storage during or after transmission, yet remains unread, could be a Title I violation. With an understanding of the nature of modern computers, a court may interpret the definition of "electronic communication" to include the storage necessary before a message is acquired by the user.[191]

Judicial interpretation should also restrict the availability of statutory exceptions. The business use exception could be held not to include computers as an excepted interception device.[192] The application of the content and context formulations of this exception may limit the employer's ability to intercept e-mail messages.[193] To provide employees with more protection, the court could restrict the service provider exceptions to reduce the number of employers who could disclaim liability.[194] The ease with which an employer can provide e-mail service is an aspect of evolving communications technology that was not considered by the drafters. A court could find that a "service provider" supplies more than e-mail within the limited context of the workplace, and require that an employer must provide e-mail and Internet access during non-work hours or from the employee's home before it can avail itself of the service provider exception.

Currently the ECPA is silent as to who may have access to the information contained within intercepted e-mail messages.[195] A court should restrict the overly broad disclosure provisions of the ECPA.[196] A court could read a requirement into the statute that disclosure may only be to parties within the business that have a valid interest in the subject matter of the message. A court could further find that disclosure to third parties outside of the business, or to those within the business that have no interest in the message, would be a violation of disclosure prohibitions under the ECPA.

C. *Statutory Reform*

Unfortunately, judicial interpretations lack the certainty, uniformity and notice of a statute.[197] Commentators are practically unanimous in calling for

---

[190] *See generally supra* notes 34-40 and accompanying text.

[191] *See generally supra* notes 41-49 and accompanying text.

[192] *See generally supra* Section III-B-2.

[193] *See generally supra* Sections III-B-2-a to –b.

[194] *See generally supra* Section III-B-1.

[195] *See* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[196] *See supra* Section IV.

[197] *See* Gantt, *supra* note 11, at 410; Note, *supra* note 5, at 1914-15 (noting the prohibitive costs of litigation, piecemeal solutions, and considerable change in judicial thinking).

statutory solutions in the form of both amendments and revisions to the ECPA or a new statutory scheme to give employees some form of privacy protection.[198] One commentator suggests that the ECPA may provide greater protection of employee interests if amended to: (1) require a legitimate business purpose for monitoring to occur; (2) remove the distinctions between "intercept," "access," and "acquire"; and (3) eliminate the outdated system provider exception.[199] Other commentators express similar proposals that require a legitimate business purpose and limit employer access to employee e-mail.[200] However, the issue of disclosure of contents of message to third parties has been left unaddressed.

Concerns about workplace privacy and the effects of changing technology on employee monitoring have recently generated legislative proposals. The Privacy for Consumers and Workers Act ("PCWA") was introduced in 1993, but failed to gain approval.[201] The PCWA proposed expanded protections to employees against monitoring to the dismay of employers.[202] The PCWA imposed a number of requirements that employers must satisfy before they may monitor employees.[203] Detailed notice, including time, date, form of monitoring, data collected, and the use of the data was to be given to both employees and non-employees.[204] Advance notice would not be required if the monitored employees were suspected of gross misconduct, unlawful activities, or conduct that adversely affects the employer.[205] Information gathered from monitoring would not be allowed in evaluation, performance, or quota

[198] *See* Droke, *supra* note 14, at 191-92 (finding the most effective route to be legislative clarification of the ECPA or creation of a new statute); Greenberg, *supra* note 8, at 247-52 (noting the irrationality of the ECPA's differing levels of protection depending on the location of the medium, and calling for legislative clarification); Note, *supra* note 5, at 1913-15 (calling for legislation specially adapted to new technologies); Rodriguez, *supra* note 17, at 1468 (stating that new legislation would offer the strongest, yet most flexible means of safeguarding employee privacy).

[199] *See* Greenberg, *supra* note 8, at 251-52.

[200] *See* Gantt, *supra* note 11, at 416 (arguing that a new federal statute should establish a "compelling business interest" standard); Lee, *supra* note 4, at 172 (calling for a flexible statute to provide for limited monitoring and decreased privacy intrusion); Droke, *supra* note 14, at 197 (calling for a statute that allow employers to search where they have good cause to believe the information will affect the pecuniary interests of the company).

[201] S. 984, 103d. Cong. (1993). This bill was sponsored in the Senate by Sen. Simon (D-Ill.). *See id.* The House bill was sponsored by Rep. Williams (D-Mont.). *See* H.R. 1900, 103d. Cong. (1993).

[202] *See* Rodriguez, *supra* note 17, at 1465; White, *supra* note 9, at 1099.

[203] *See* Lee, *supra* note 4, at 167-68; White, *supra* note 9, at 1100.

[204] *See* S. 984, §§ 4(b), 5(B)(3); Lee, *supra* note 4, at 167-68; White, *supra* note 9, at 1100.

[205] *See* S. 984, § 5(c)(1); Lee, *supra* note 4, at 168; White, *supra* note 9, at 1101.

reviews.[206] The PCWA proposed a controversial "tiered" approach to monitoring that called for different levels of monitoring according to employee seniority.[207] This aspect that was criticized as too inflexible to adapt to employer needs and concerns.[208] However, the PCWA has been praised for employee empowerment and recognition that excessive monitoring may be adverse to both employer and employee interests.[209]

One commentator finds fault in the PCWA because it "eliminates the surreptitious nature of employer monitoring without effectively restricting the scope of the monitoring."[210] Gantt argues that legislation must abandon the focus on employees' expectations of privacy and employers' interest in monitoring.[211] Instead, he argues we must recognize privacy as an independent right and require employers to justify any intrusions into employee privacy.[212]

Legislation tailored to reduce the intrusions into employee privacy caused by monitoring is sorely needed. However, proposals to restrict disclosure have been an ignored aspect of employee e-mail privacy legislation. Even the most restrictive monitoring policy will fail to achieve its goal of reduction of privacy intrusion if it does not limit the disclosure of intercepted messages. Without a valid restriction on disclosure, the employee may face not only punishment from the company if the e-mail violated company policy, but also humiliation, embarrassment, and invasion of privacy if the e-mail is disclosed to colleagues or made public. Legislative proposals regarding e-mail privacy within the workplace must contain a clause restricting disclosure.

This note proposes an amendment to the ECPA that consists of a section to specifically address the proper scope of disclosure. In the event of an improper interception, there should be an absolute ban on disclosure of the e-mail contents to any person other than the intended recipient. For properly intercepted messages, disclosure should be limited to parties within the company who can demonstrate that they have a valid business interest in the subject matter of the message. Under this standard, personal information in an e-mail message is not to be disclosed, only the information that pertains to business operations. Disclosure of business-related information to third parties, outside of the company, should be limited to those persons with a compelling business interest. Personal information contained within a properly

---

[206] *See* S. 984, § 8(b).

[207] *See id.* § 5(b); Rodriguez, *supra* note 17, at 1464-65.

[208] *See* Gantt, *supra* note 11, at 409 (noting that the "tiered" approach increases privacy for workers with seniority, but creates unreasonable obstacles to legitimate employer monitoring); Lee, *supra* note 4, at 171 (explaining that the PCWA is too inflexible to adapt to monitoring in different business contexts); Rodriguez, supra note 17, at 1465.

[209] *See* Flanagan, *supra* note 8, at 1279-81.

[210] Gantt, *supra* note 11, at 409.

[211] *See id.* at 411-12.

[212] *See id.* at 412.

intercepted e-mail message should never be disclosed to third parties. However, an employee may authorize the disclosure of a specific message's content with express, informed consent. This consent must be obtained separately for each disclosure.

The statute should allow for recovery for actual damages and any profits made by the disclosing party from the disclosure. As it may be hard to prove actual damages, and the disclosing party may not have made money by the disclosure, the statute should provide for statutory damages in order to ensure the existence of an adequate deterrent. Finally, the statute should provide for punitive damages in cases where the judge may see fit; for example, an incredibly damaging personal disclosure, or a continual violation of an employee's privacy. The following is the text of the proposed addition:

Section 2800. Disclosure of Electronic Communications

(a) This section shall apply to the interception of any electronic communication under both Title I and Title II of the ECPA that is not made during a continuing criminal investigation.

(b) Disclosure of the contents of any electronic communication to any party other than the intended recipient is strictly prohibited if intercepted in violation of any sections of the ECPA.

(c) For electronic communications that are intercepted without violation of any provisions of the ECPA or are exempted from violation by satisfaction of an exception, the contents may be disclosed to:

(1) the sender or intended recipient;

(2) supervisors employed by the intercepting employer who have a valid business interest in the information contained within the electronic communication;

(3) a third party, upon the showing by the employer of a compelling business interest in the contents of the message;

(4) a law enforcement agency if the contents pertain to the commission of a crime.

(d) Disclosure of personal, non-business related contents of a properly intercepted electronic communication to any party other than a law enforcement agency, if the contents pertain to the commission of a crime, is strictly prohibited.

(e) The limits on disclosure provided by subsection (c) and (d) may be waived by the sender or recipient through express written, informed consent to each episode of disclosure.

(f) The damages available include the following:

(1) punitive damages in cases where appropriate or if the defendant is a repeat violator of this section; and

(2) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(3) statutory damages in the amount of $1,000 for each incident of disclosure in violation of this section.

(g) This section shall not limit disclosure to any party of the transactional components of an electronic communication, such as sender, recipient, date, or length of message.

This proposal for restrictions on disclosure would best serve the employee's interest in maintaining privacy of personal information contained within e-mails, as well as the employer's interest in employee monitoring and business-related information. This section would serve to protect employees from disclosure regardless of the technology involved. More importantly, this section provides protection regardless of the legitimacy of the underlying interception. Therefore, employee privacy interests against unrestricted disclosure are no longer dependant on the application and interpretation of the underlying statute.

VI. CONCLUSIONS

Current law fails to adequately protect worker privacy rights. With the rate at which e-mail and other forms of electronic communications are advancing, the current framework leaves employees subject to having their e-mail intercepted and discussed with whomever the employer chooses. It is argued that too much depends on outdated thinking about technology and employee privacy interests.[213] Some commentators focus on the liability employers may face due to invasions of privacy, arguing that the statutory language needs to be cleared up in order to offer the employer guidance.[214] However, others warn that the law is too protective of employer interests and leaves employees "at the mercy of employers who take an active role in browsing

through their E-mail."[215] Employees need certainty about their protection in the workplace and employers need certainty that their actions will not incur liability. In order to achieve this balance there must be a combination of employer initiatives to control and limit e-mail monitoring and disclosure, as well as statutory clarification in the form of interpretation and new legislation in light of evolving technology and employee privacy concerns.

---

[213] *See* Greenberg, *supra* note 8, at 253.

[214] *See, e.g.*, White, *supra* note 9, at 1102.

[215] Lee, *supra* note 4, at 169.