Pacific Northwest National Laboratory

Operated by Battelle for the
U.S. Department of Energy

Legal and Policy Issues Associated with Monitoring Employee E-mail

M.A. Segura
A.C. Rither

January 1997

RECEIVED
FEB 06 1997
OSTI

Prepared for the U.S. Department of Energy
under Contract DE-AC067-76RLO 1830

PNNL-11447

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY

operated by

BATTELLE

for the

UNITED STATES DEPARTMENT OF ENERGY

under Contract DE-AC06-76RLO 1830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831;
prices available from (615) 576-8401.

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161

This document was printed on recycled paper.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Legal and Policy Issues Associated with Monitoring Employee E-mail

M.A. Segura
A.C. Rither

January 1997

Prepared for the U.S. Department of Energy
under Contract DE-AC067-76RLO 1830

Pacific Northwest National Laboratory
Richland, Washington 99352

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

EXECUTIVE SUMMARY

This paper examines the legal issues involved with employer monitoring of employee e-mail. In addition to identifying pertinent legal issues, the paper provides guidelines that will help the Pacific Northwest National Laboratory (PNNL) establish a program for monitoring outgoing e-mail to insure compliance with company policies, particularly those regarding protection of trade secrets and proprietary information, and to comply with the Department of Energy's (DOE) procedures for protecting Export Controlled Information (ECI).

Electronic communication has allowed companies to enhance efficiency, responsiveness and effectiveness. E-mail allows employees to transmit all types of data to other individuals inside and outside of their companies. The ease with which information can be transmitted by e-mail has placed trade secrets, proprietary information, and other sensitive data at risk from inadvertent disclosure by employees. As employers attempt to protect their interests through measures such as monitoring e-mail, they may expose themselves to liability under federal and state laws for violating employee privacy. Business use of e-mail has proliferated so rapidly that the federal and state legal systems have not been able to adequately address the issues arising out of its use in the workplace.

The primary legal issues associated with e-mail monitoring are reasonable expectation of privacy, legitimate business interests, the existence of e-mail policies, and employee consent to e-mail monitoring. Since e-mail monitoring by employers is still an evolving area of the law, there are many uncertainties about the scope of federal and state privacy statutes and their interpretation by the courts. E-mail monitoring issues involving federal law are most likely to be adjudicated under the Electronic Communications Privacy Act of 1986 (ECPA). Cases involving federal agencies or their contractors may sometimes fall under the Fourth Amendment to the U.S. Constitution. State law cases may be adjudicated under common, constitutional, or state statutory law.

The ECPA expressly protects electronic communications. Although the ECPA does not specifically mention e-mail, the Act's definition of electronic communication appears to encompass e-mail. Most commentators believe that the legislative history indicates that Congress intended to include e-mail within the scope of the ECPA's protection. This view has been supported by one federal court. The extent to which the ECPA actually protects employee e-mail from employer monitoring is unclear.

The Act contains three exceptions which may exempt employer's from the its provisions. The federal courts have interpreted these exceptions in relation to telephone monitoring but not to e-mail. The "employer provider" exception may exclude private employers who provide e-mail systems through intracompany networks. A California court has indicated in dictum that employer-providers would be exempt under the ECPA's provider exemption. The scope of this exception is uncertain, but many commentators believe that, by itself, the employer-provider exception may provide only a limited right for employers to monitor e-mail. These commentators recommend that an employer should adopt a formal e-mail policy and communicate that policy to

its employees. A published e-mail monitoring policy may be used by an employer to show that the purpose of the monitoring is to protect the employer's legitimate business interests or property rather than to invade the privacy of its employees.

The ECPA's "business use" exception appears to provide exemptions for employers if employee communications are accessed in the ordinary course of business. Whether an employer is exempted by this exception may depend on whether the employer is able to articulate legitimate business interests to justify monitoring employee communications and has given notice of the monitoring to the employees. Some commentators believe this exception allows an employer to monitor employee communications only to the extent necessary to determine whether they are business or personal. A second provision of the business use exception appears to allow employers and authorized employees to monitor electronic communications if necessary and incidental to providing the service or protecting the employer's property rights. These property rights include preventing system failure, protection of trade secrets and proprietary information, and avoidance of liability. Many commentators believe that a court will attempt to balance the legitimate business interests of the employer against an employee's reasonable expectation of privacy in his or her e-mail. Most commentators recommend that an employer wishing to minimize its potential liability should go further than merely relying on the weight of its business interests and obtain employee consent.

Under the "prior consent" exception, the ECPA allows interception of electronic communications where one of the parties to the communication has given prior consent. The courts in the telephone monitoring cases have held that consent may be either express or implied, but constructive consent is not valid. Most commentators recommend that the best way to obtain consent is through a well-defined e-mail policy that is communicated to the employees.

Two federal court cases that involve employer monitoring of employee e-mail have been reported. The first, addressed access to stored electronic communications under the ECPA and the Fourth Amendment. The court equated the employer's system to e-mail, and held that under the ECPA, the provider of a communication service could do as it wished when accessing stored electronic communications. Under the Fourth Amendment privacy claim (the employer was a government entity), the court held that the employees failed to demonstrate a reasonable expectation of privacy in their communications because they had been warned that the communications were not private, and the employer routinely recorded its communications during its ordinary course of business.

The second federal court case was tried under a state common law action of invasion of privacy. The court balanced the employee's privacy interest against the employer's legitimate business interests, and found that the employee did not have a reasonable expectation of privacy to e-mail communications that he voluntarily made over his employer's e-mail system. The court added that even if it had found that the employee had a reasonable expectation of privacy, that interest would have been outweighed by the employer's interest in preventing inappropriate comments or illegal activity over its e-mail system.

The first federal case mentioned above has been the only case to consider an employer e-mail monitoring issue under the Fourth Amendment. The Fourth Amendment applies, in this context, only to government employers or their agents. It does not apply to private employers acting alone to protect their legitimate business interests. Even government employers are not constrained by the Fourth Amendment when conducting administrative searches of an employee's exclusive use area if the search has been initiated for a legitimate business purpose and not for the purpose of obtaining evidence of criminal prosecution. Evidence of criminal conduct discovered incidental to an administrative search may be turned over to law enforcement authorities for prosecution by the employer.

The Revised Code of Washington (RCW) 9.73.030 prohibits interception, recording, and divulging private communications by individuals, businesses, and governmental agencies. Although the statute does not specifically refer to e-mail, a bill, which would have amended RCW 9.73.030, was introduced in the Washington House of Representatives that expressed a legislative intent to address privacy concerns relating specifically to e-mail and other electronic communications. RCW 9.73.030 contains an exception for prior consent as long as it has been given by all the parties. Implied consent is sufficient as long as notification is given to all parties that the communication is about to be recorded and the notification is included on the recording. Washington courts have applied RCW 9.73.030 to telephone monitoring by the police, but have not yet applied it to e-mail. The courts have noted that RCW 9.73.030 is more restrictive than the ECPA, but they have also noted that it protects only "private communication," which is not defined in the statute. The courts have stated that private communication will be interpreted considering the expectations of the parties under the circumstances of each case. An appropriate e-mail monitoring policy and effective notice to employees could be used by an employer to argue that office e-mail is not a type of communication to which employees have a reasonable expectation of privacy and, therefore, is not private under RCW 9.73.030. California has a privacy statute similar to Washington's. Several California courts have decided privacy suits in favor of employers based on a lack of employee expectation of privacy and because the language of the statute did not encompass e-mail.

Washington recognizes a common law action for invasion of privacy, but it is not clear whether an employee could demonstrate that e-mail monitoring is a substantial invasion of privacy that is offensive and objectionable to an ordinary person. The federal e-mail case, decided under another state's common law using the same standard, failed to find that e-mail monitoring was sufficiently invasive or offensive. A California court has rejected an e-mail monitoring claim because the employees signed a business use acknowledgment and had actual knowledge that their e-mail was being monitored by their employer.

Washington courts have found that the state's constitutional privacy article is more restrictive than the Fourth Amendment of the U. S. Constitution, and that the state has extended strong protections to electronic communications. However, the article applies only to government action. A Washington court, in a constitutional privacy case, would likely give considerable weight to an

employee's reasonable privacy expectations, but it would also weigh the competing legitimate interests of the employer.

Until the legal parameters of e-mail monitoring by employers is more clearly defined, an employer who wants to reduce its potential liability should establish a well-drafted and clearly-defined company e-mail policy that is communicated to its employees. These policies must define the employer's rights and expectations, inform employees that e-mail is for business purposes only, warn employees that the employer monitors e-mail for business purposes, and advise employees that the employer can access any password or message at any time. A company e-mail policy may be established as a separate policy or as part of a general electronic communication policy. The policy should be tailored to the workplace environment, and should be consistent with federal and state laws. PNNL should ensure that employees are aware of the types of information that are considered proprietary or trade secrets. PNNL should also inform employees about the requirements for protecting ECI. Employees should be told that e-mail is being monitored as part of PNNL's information protection program. Employees may be notified of e-mail policy by one or more of the following methods: publication in the company's policy manual, a briefing during new employee orientation and annually thereafter, or as an annual information security reminder transmitted electronically to all employees over the intracompany network.

CONTENTS

Executive Summary	iii
1. Introduction	1.1
2. Electronic Privacy Act of 1986	2.1
3. Federal Court Decisions on Monitoring Employee E-mail	3.1
4. The Fourth Amendment E-Mail Monitoring by the Government or Its Agents	4.1
5. E-mail Monitoring under State Law	5.1
6. E-mail Monitoring Policy and Notice Considerations	6.1

1. INTRODUCTION

This paper examines the legal issues associated with monitoring by an employer of employee e-mail messages transmitted over a system it provides employees for use in conducting company business. The purpose of this paper is to identify issues and provide guidelines that will assist the Pacific Northwest National Laboratory (PNNL) to establish a program for monitoring outgoing e-mail to insure compliance with company policies, particularly those regarding protection of trade secrets and proprietary information, and for minimizing the risk of dissemination of Export Controlled Information (ECI).¹

Electronic communication technology has become an essential tool for modern business. Companies large and small are able to transmit technical, scientific and other business documents internationally in an instant. Employees are linked with each other through internal computer networks and with outside entities through the Internet. Of all the forms of electronic communication in the workplace, e-mail has proliferated the fastest. In fact, it has grown so rapidly that the law has not yet kept pace with the issues relating to employer and employee rights arising from its use. The ease and speed at which information can be transmitted by e-mail has made it harder for employers to protect trade secrets, proprietary information, and other sensitive data from inadvertent disclosure by careless employees. As employers institute safeguards, such as e-mail monitoring, to protect their business interests, they may expose themselves to liability for violating employee privacy when monitoring is done without their consent. Most commentators believe that unnecessary litigation can be avoided by establishing a company e-mail policy and informing the employees of what the company considers appropriate and inappropriate uses of the e-mail system.²

The e-mail monitoring issues identified in this report are discussed in terms of federal and state law. Since PNNL is located in Washington State, the discussion of pertinent state law issues is focused on Washington law. Washington, along with other states, is just beginning to address e-mail monitoring, and e-mail monitoring as a specific concern has not yet been addressed by the

legislature or the courts. The following are the primary issues associated with e-mail monitoring in the employment context: 1) employee privacy expectations, 2) legitimate employer interests, 3) existence of a company e-mail policy, and 4) employee consent. The issues and the approach to analyzing them are fairly consistent among the various jurisdictions. Therefore, this paper should be helpful to other national laboratories in formulating their own e-mail monitoring policies and programs. Nevertheless, each national laboratory should research the e-mail or electronic communications law of the particular state in which it is located, as well as the law of each state in which it maintains facilities and staff. Each laboratory should establish its own e-mail policy consistent with state and federal law and tailored to its particular workplace environment and security interests.

The first three sections of this paper examine e-mail monitoring under the following aspects of federal law: the Electronic Communications Privacy Act of 1986 (ECPA), federal court cases interpreting the ECPA and e-mail monitoring by employers under the Act and under Pennsylvania law, and the Fourth Amendment to the U.S. Constitution as it relates to government employers and their agents. The fourth section of the paper discusses e-mail monitoring under Washington State law. The fifth section presents guidelines for formulating company e-mail policy.

ENDNOTES

INTRODUCTION

1. Export Controlled Information (ECI) is a term used to designate unclassified U.S. Government information over which the Department of Energy (DOE) has authority, which if released, could reasonably be expected to adversely affect U.S. national security or nuclear nonproliferation objectives. Exportation of ECI by the private sector requires a Department of Commerce or Department of State validated license or a DOE authorization for export under U.S. laws or regulations.
2. Laurie Thomas Lee, "Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop,'" 28 J. Marshall L. Rev. 139, 172-73 (1994); Donald H. Seifman and Craig W. Trepanier, "E-mail and Voicemail Systems. Evolution of the Paperless Office: Legal Issues Arising Out of Technology in the Workplace, Part 1," 21 Empl. Rel. L. J. 3, at 5 (1995); and Perkins Coie, "Even the Rose of Communication Has Some Thorns," 2 Wash. Empl. Law Letter 3, at 1 (April 1995).

2. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

The Electronic Communications Privacy Act of 1986 (ECPA)¹ has been interpreted to give federal statutory protection to e-mail. The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968² (the federal wiretap law) to expressly protect electronic communications.³ While the ECPA's definition of electronic communication would appear to encompass e-mail transmissions, the Act does not directly mention e-mail. Nevertheless, many commentators believe the legislative history indicates that Congress specifically intended to include e-mail within the scope of the ECPA's protection.⁴ This view has been supported by the United States District Court for the District of Nevada in the only reported federal court decision to date which has discussed the application of the ECPA to e-mail monitoring by an employer.⁵

The ECPA prohibits unauthorized interception of electronic communications as well as disclosure or use of that information.⁶ The ECPA also protects against unauthorized access to stored communications, as well as the disclosure and use of information derived therefrom.⁷ The Act prescribes civil damages and criminal penalties for violations of its provisions.⁸

While most commentators believe that Congress clearly intended for the ECPA to protect an individual's privacy interest in his or her personal e-mail, many believe that the extent to which the Act protects an individual in his or her capacity as an employee from e-mail monitoring by his employer is unclear.⁹ The scope of the ECPA's protection of an employee's e-mail from employer monitoring is likely to depend on judicial interpretation of the following three exceptions to the Act's prohibitions.

Employer Owned/Provider Systems Exception

The ECPA provides an exception for electronic communications systems providers from the Act's prohibitions on interception¹⁰ of electronic communications and access to and disclosure

of stored communications.¹¹ An absence of case law interpreting the exception makes predicting its application to private employers uncertain. Several commentators believe that ECPA prohibitions may apply only to employers who provide e-mail service through public networks such as Internet, CompuServe, and Prodigy. Although they feel the ECPA is unclear on this point, they believe that the systems exception may exclude private employers who provide e-mail systems through intracompany networks from ECPA liability because they may not be transmitting electronic communications that "affect interstate or foreign commerce" as defined in the Act.¹² A California superior court decision relating to e-mail interception under the state's wiretap statute discussed the ECPA exception in a footnote, and indicated in dictum that employer-providers would have been exempted from the Act's prohibitions.¹³ Nevertheless, another commentator states that this reasoning "ignores Congress' stated intent to procure parity in the protection of personal communications, regardless of the medium of transmission."¹⁴ She states that "an employer who [interprets the ECPA as allowing an employer the unlimited right to access and disclose its employees' private e-mail communications, or that the Act was simply not intended to cover employers at all] does so at its own peril."¹⁵ She suggests that "at a minimum ... [an employer must] inform the individual user of company policy regarding 'the uses and disclosure of personally identifiable information.'" A prudent employer should examine what the courts have considered reasonable employee expectation of privacy for things other than e-mail, such as an employer's legitimate business need to examine an employee's regular mail and phone calls.¹⁶

Assuming that employer owned e-mail systems are covered by the ECPA, an employer has at least a limited right to intercept employee e-mail communications transmitted over or to access e-mail stored on the employer provided system.¹⁷ Based on that assumption, it would be prudent for PNNL to adopt this point of view in relation to e-mail monitoring for purposes of protecting its own trade secrets and proprietary information, as well as ECI. Guidelines for a corporate e-mail monitoring policy and employee notice requirements are discussed in the last section of this paper.

Business Use Exception

An employer's right to read and disclose the content of employee e-mail without obtaining employee consent may depend on whether the employer has intercepted the communication or accessed stored data. Two sections of the ECPA provide possible exceptions for interceptions conducted in the ordinary course of business. One has been referred to as the business telephone extension exception and the other as the property protection exception.

Section 2510(4)(5) defines "intercept" as the use of an electronic, mechanical, or other device to access the contents of communications, but specifically excludes from the definition of electronic device, telephones or telephone equipment furnished to a user and being used in the ordinary course of business by either the user or the service provider.¹⁸ One commentator suggest that the exception may not apply to e-mail unless "telephone" equipment and facilities are actually used, and that it is unclear whether a court would consider a "network manager's modem, computer, or software program to be telephone ... equipment."¹⁹ While the courts applied this exception to exempt employer telephone monitoring using business telephone extensions, they have yet to apply it to e-mail interception.²⁰

One approach used by the courts in telephone extension cases emphasizes the employment related circumstances surrounding the workplace monitoring. These circumstances include whether the employer is able to articulate legitimate objective business considerations to justify the monitoring and whether the employer has notified employees that their communications could or would be intercepted.²¹ The other approach focuses on the content of the communication. Under this approach, an employer may intercept employee communications only to the extent necessary to determine whether they are business or personal, but the employer may not examine the content of personal communications.²² Considering the telephone extension cases, several commentators urge caution when relying on a

"communications device" exception. They suggest that the safest course would be to limit e-mail monitoring to transactional information, such as sender, receiver, message headings, and elapsed transmission time/length of message, for peculiarities that may objectively indicate abuse of the system or compromise of the employer's legitimate business or property interests. Other commentators suggest that this approach may not be practical, and there is little indication from the few cases that have involved e-mail monitoring that an employer protecting its legitimate business interests would be required to restrict its access only to transactional information.²³ This is especially true if the employer has established a formal e-mail policy, and has communicated that policy to its employees.

Section 2511(2)(a)(I) allows an electronic communications service provider or its authorized employees to intercept certain electronic communications during the normal course of business if necessary in order to render the service or to protect the provider's rights or property.²⁴ The intercepting employee must be acting within the scope of his or her employment, and the purpose must be necessary and incidental to providing the e-mail service, such as system maintenance or protecting the employer's property rights, which may include prevention of system failure, protection of trade secrets and proprietary information, avoidance of liability for tortious conduct (libel, defamation, harassment, discrimination, copyright infringement), and discovery of unauthorized personal use.²⁵ Attempting to anticipate the judicial application of this exception to e-mail, some commentators have cited broad judicial interpretations of this exception in relation to telephone monitoring; however, others suggest that the courts may construe the exemption narrowly.²⁶ In applying these ECPA exceptions to e-mail, the courts are likely to use the same type of analysis as they do in Fourth Amendment and tort privacy cases, which is a balancing of the legitimate privacy interests of the employee against the legitimate business interests of the employer.

E-mail and other types of electronic communications systems have made it increasingly difficult for employers to protect their trade secrets and other sensitive business information from unauthorized disclosure by employees.²⁷ Still, PNNL should be prudent and approach the

business use exceptions conservatively. Regardless of the possible differences in judicial interpretation, obtaining employee consent to e-mail monitoring would avoid many of the legal uncertainties, and could legitimize monitoring activities that might otherwise be considered legally impermissible.²⁸

Prior Consent Exception

The ECPA allows interception of electronic communications "where one of the parties to the communication has given prior consent, as long as the monitoring is not conducted for an unlawful purpose."²⁹ Stored information may also be accessed by consent of the intended recipient of the communication.³⁰ Applying the consent exception to telephone monitoring cases, the courts have held that consent may be either express or implied.³¹ Implied consent may be inferred from the circumstances.³² Constructive consent, "knowledge of the capability of monitoring alone" or that a person "should have known" that monitoring was a possibility, does not amount to valid consent.³³

In order to ensure valid employee consent, PNNL should publish specific policy concerning employee use of PNNL and DOE provided electronic communications systems and equipment. Additionally, PNNL should notify employees in writing that e-mail and other electronic communications systems are being monitored to protect PNNL and DOE legitimate legal interests. One commentator offers the following guidelines:

[A]n employer who needs to monitor employee E-mail use should disseminate a comprehensive policy statement defining the circumstances under which monitoring will occur. The policy should define the employer's ability to monitor, so that passwords, varying levels of message protection, and other security measures will not mislead the employee into believing that at least some messages are beyond the employer's reach. To ensure that the appropriate consent has been given, abide by the limits set by that policy.³⁴

Another commentator concurs and suggests that the reasoning by the courts in the telephone

monitoring cases "implies that employers will escape liability if they publish a comprehensive monitoring policy," and believes that after an employer publishes an e-mail monitoring policy, "an employee's continued use of the e-mail network will presumably constitute, at a minimum, consent to employer interception of work-related messages and personal messages to the extent needed to determine whether the messages are personal or business in character."³⁵ Rather than rely on implied consent through "continued use," an employer might consider incorporating its monitoring policy into a written form that employees would sign acknowledging that they have read the policy and have agreed to abide by it.³⁶ All new employees would execute the forms as part of their initial orientation and in-processing. An employer might also consider displaying a warning about the business nature of e-mail use containing a reminder about e-mail monitoring. Employers should be sensitive to employee concerns, since publishing an e-mail monitoring policy and requiring employees to sign acknowledgment statements or compliance agreements may negatively impact employee morale.³⁷

A published e-mail monitoring policy may be used as proof that the purpose of the monitoring is to protect PNNL property and other legitimate business interests rather than to intrude on the privacy of its employees. However, once an employer publishes a monitoring policy, it is bound by the limits of that policy and must adhere to it.³⁸

ENDNOTES
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

1. 18 U.S.C. 2510-2521, 2701-2710, 3117, 3121-3126
2. 18 U.S.C. 2510-2520
3. 18 U.S.C. 2510(12) defines electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include - (A) any wire or oral communication. . .," as defined by 18 U.S.C. 2510(1) and (2) as an "aural transfer." An aural transfer is a communication that contains the "human voice...." 18 U.S.C. 2510(18).
4. "Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences." S. Rep. No. 541, 99th Cong., 2nd Sess. 14 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556 and cited by Paul E. Hash and Christina M. Ibrahim, "Selected Topics on Employment & Labor Law: E-Mail, Electronic Monitoring, and Employee Privacy," 37 S. Tex. L. Rev. 893, 898, n32 (1996); Larry O. Natt Gantt, II, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace," 8 Harv. J. Law and Tec. 345, 351, n45 at 352 (1995); and Ruel Torres Hernandez, "ECPA and Online Computer Privacy," 41 Fed. Com. L.J. 17, 28-29, n43-44 (1988). See also Julia T. Baumhart, "The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?" 8 Lab. Law. 923, 924-25 (1992), stating that "E-mail, a data processing system that employs communications technology to transmit mail in electronic form, undoubtedly is a form of electronic communication, as is its commonly used counterpart, computer-to-computer communications."
5. *Bohach v. City of Reno*, 923 F. Supp. 1232 (D. Nev. 1996), in which the judge stated that alphanumeric (non-voice) messages, transmitted over a police department's Local Area Network (LAN) via Alphapage Media Notification System Software and stored on the department computer system's Inforad Message Directory, were "essentially electronic mail" which were "'electronic' communications within the meaning of 18 U.S.C. 2510(12)."
6. 18 U.S.C. 2511(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 an endeavor to intercept, any wire oral, or electronic communication;... (c) intentionally discloses, or endeavors to disclose, to any person the contents of any wire, oral, or electronic communication;... or (d) intentionally uses, or endeavors to use, the

contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection ... shall be punished and provided in subsection (4) or shall be subject to suit as provided in subsection (5)." 18 U.S.C. 2510(4) defines intercept as "the aural or other acquisition of the contents of any wire, electronic, mechanical, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. 2510(17) defines electronic storage as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. 2510(15). An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications."

7. 18 U.S.C. 2701(a). "Except as provided in subsection (c) of this section whoever - (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section." 18 U.S.C. 2510(14). An electronic communications system is defined as "any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. 2702(a). "Except as provided in subsection (b) - (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service...."
8. See Gantt, *supra* note 4, at 353. Gantt outlines the authorized civil damages and criminal penalties - "A civil plaintiff who proves a violation of the interception provisions may recover the greater of either: (1) actual damages suffered and any profits made by the violator; or (2) statutory damages the greater of \$100 a day for each day of violation or \$10,000. 18 U.S.C. 2520(c)(2). A successful plaintiff may also recover reasonable attorneys' fees, litigation costs, and other equitable relief. 18 U.S.C. 2520(a)(3). The criminal penalty for interception violations includes up to five years imprisonment and fines up to \$500. 18 U.S.C. 2511(4)(a)-(b). A civil plaintiff who proves a violation of the stored communications provisions may recover equitable relief, damages including lost profits with a damage minimum of \$1000, and reasonable attorneys' fees and litigation costs. 18 U.S.C. 2707(a)-(c). The criminal penalty includes up to one year imprisonment and fines up to \$250,000 on the first offense if the offense is committed for commercial advantage or involves malicious destruction or damage or private commercial gain. 18 U.S.C. 2701(b)." Baumhart, *supra* note 4, at 936 states that "damages are the only

remedies available for ECPA violations involving electronic communications...,” and the courts begin by assuming that “only actual loss is compensable in individual privacy claims.”

9. Gantt, *supra* note 4, at 352. Gantt notes that “the ECPA does not explicitly offer protection from employers who access or intercept the electronic communications of their employees. He states that “Congress was primarily concerned about protecting corporations against their competitors that might desire to steal valuable electronic information”, and indicates that the ECPA provisions apply to the unauthorized acts of employees and individuals outside the company. He also notes the lack of “any clear congressional intent [in the legislative history] that the Act should not be read to cover private employer monitoring of employee E-mail.” See Baumhart, *supra* note 4, at 925 (citing S. Rep. No. 541, 3-4, 1986 USCCAN 3557-58). Baumhart states that the Senate Report underscores “individual privacy concerns as the primary reason for including E-mail and similar forms of electronic communications” in the ECPA based on the report’s assertion that “‘electronic mail remains legally as well as technically vulnerable to unauthorized surveillance’.” While Baumhart believes Congress “clearly intended to provide broad privacy protection to individuals..., she thinks “it is less clear to what extent, or even whether Congress intended to protect the individual in his capacity as an employee from privacy invasions by his employer.”
10. 18 U.S.C. 2511(2)(a)(I). “It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.”
11. 18 U.S.C. 2701 (c)(1)(2). “Subsection (a) of this section does not apply with respect to conduct authorized - (1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. 2702(b). A person or entity may divulge the contents of a communication ... (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; [or] (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service....”
12. See Donald H. Seifman and Craig W. Trepanier, “E-mail and Voicemail Systems. Evolution of the Paperless Office: Legal Issues Arising out of Technology in the Workplace, Part 1,” 21 Employee Relations L. J. 3, page 5 (1995); and Laurie Thomas Lee, “Watch your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the Electric Sweatshop,” 28 J. Marshall L. Rev. 139 (1994). Both articles citing 18

U.S.C. 2510(12).

13. Gantt, *supra* notes 4, at 359. (Citing *Flanagan v. Epson America, Inc.*, No. BC007036, slip op. at 5-6 n.1 (Cal. Super Ct. Jan. 4, 1991), in which the court stated that "there simply is no ECPA violation if 'the person or entity providing a wire or electronic communications service' intentionally examines everything on the system." (quoting *Hernandez*, *supra* note 4, at 39.)
14. Baumhart, *supra* note 4, at 927-928. Baumhart states that since "Congress expressly intended that pre-ECPA prohibitions apply to employers who intercept employee telephone conversations;... it is feasible that Congress saw no need to specify that ECPA coverage [for electronic communications such as e-mail] likewise extends to employers. Baumhart cites Senate hearing testimony on the ECPA which he claims demonstrates specific intent that "all electronic communications, including ... internal company-owned E-mail systems" be covered by the Act, and that "absent 'positive signals' to the contrary, E-mail users 'generally [have] an expectation of privacy,' which should be legally enforceable." (Citing Hearing on S 1667 99-100 and 147; See also Gantt *supra* note 4, at 362.
15. Baumhart, *supra* note 4, at 928 and Gantt, *supra* note 4, at 363, suggesting that the ECPA provision allowing providers to access stored data was intended specifically to allow providers to perform systems maintenance and to back-up or restore messages. See also 18 U.S.C. 2701(c)(1)(2) and 2702(b)(4)(5), *supra* note 11.
16. Baumhart, *supra* note 4, at 929. Baumhart suggests that storing messages as "'back-up files' longer than administratively necessary may imply a true purpose more invasive than back-up...." This caution should not apply as long as the stored files serve a legitimate business need, and the employer is able to demonstrate the business interest served by maintaining the files.
17. *Id.*, *supra* note 4, at 925; See also Gantt, *supra* note 4, at 363.
18. 18 U.S.C. 2510(4). "[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any wire, electronic, mechanical or other device." 18 U.S.C. 2510(5). "[E]lectronic, mechanical or other device' means any device or apparatus which can be used to intercept a wire, oral or electronic communication other than - (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the...user by a provider of wire or electronic communication service in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business...."
19. Lee, *supra* note 12, at 155.

20. Gantt, *supra* note 4, at 364-65
21. *Id.*, at 365-67. (Citing *United States v. Harpell*, 493 F.2d 346 (10th Cir. 1974) in which the court held an employer's telephone interception was illegal because of inadequate employee notice of workplace monitoring, and therefore, lack of consent. Also citing *James v. Newspaper Agency Corp.*, 141 F.2d 579, 581 (10th Cir. 1979), upholding an employer's installation of a device to monitor employee's business calls. The court emphasized that the monitoring had been fully disclosed to the employees, none of whom objected. In addition, the reasons for monitoring stated by the employer, which included protection from abusive calls and facilitation of employee training and instruction by supervisors, were legitimate business purposes. Gantt also cited *Deal v. Spears*, 980 F.2d 1153 (8th Cir 1992), for the proposition that even when a legitimate business interest exists, extended general surreptitious monitoring including personal calls, the content of which has no relation to the employers business interest, was outside the scope of the exception.)
22. *Id.*, at 367-369. Citing *Watkins v. LM Berry & Co*, 704 F.2d 577 (11th Cir. 1983) in which the court stated that monitoring employee "personal calls is never 'in the ordinary course of business...except to the extent necessary to guard against unauthorized use or determine whether a call is personal or not'," and the "'ordinary course of business'" does not include "'anything that interests the company.'" Also citing, *Briggs v. American Filter, Co.* 630 F.2d 414 as an example of a more liberal interpretation "explicitly rejecting the idea that non- consensual interception is never allowed." The court considered that an employer who monitored a call in which an employee disclosed trade secrets to a competitor acted within the ordinary course of business. The court noted that the employer legitimately suspected that its business interests were being compromised and used the extension phone to monitor only the business portion of the call. The court indicated that it might have ruled differently had the employer monitored a personal portion of the call or had engaged in general surreptitious monitoring. See also Lee, *supra* note 12, at 156-57.
23. Baumhart, *supra* note 4, at 933-34. Suggesting that the courts are likely to be more receptive to transactional rather than to content monitoring, especially if the content of some of the communications may be personal. See also Gantt, at 370.
24. 18 U.S.C. 2511(2)(a)(I), *supra* note 10.
25. Lee, *supra* note 12, at 156. See also Baumhart, *supra* note 4, at 930-31.
26. *Id.*, Lee at 156; and Baumhart, at 931-32. Noting that although application of this exception by the federal courts "is virtually non-existent" (as of 1992), and that the pre-ECPA statute expressly limited random monitoring to quality control checks, she cautions that the "treatment of the pre-ECPA exception and the similar 'business extension' exemption, suggests that the exemption will be narrowly construed." She suggests the

courts may look for minimal intrusion into content, and interception of only "that which [is] essential to protecting the [employer's legitimate] property interest. (Citing *United States v. Beckley*, 259 F. Supp. 567 (ND Ga 1965); *United States v. Clegg*, 509 F.2d 605 (5th Cir. 1975); and *United States v. Ross*, 713 F.2d 389 (8th Cir. 1983).)

27. Seifman and Trepanier, *supra* note 12.
28. Baumhart, *supra* note 4, at 930. See also Gantt, *supra* note 4, at 370.
29. 18 U.S.C. 2511(2)(d). "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 a person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."
30. 18 U.S.C. 2701(c)(1)(2). "Subsection (a) of this section does not apply with respect to conduct authorized ... (2) by a user of [the electronic communications] service with respect to a communication of or intended for that user."
31. Gantt, *supra* note 4, at 355. Citing *Griggs-Ryan v. Connelly*, 904 F.d. 112 (1st Cir. 1990).
32. Lee, *supra* note 12, at 153, n73. Citing *Griggs-Ryan*, 904 F.2d 112, 117, in which the court, quoting *United States v. Amen*, 831 F.2d 373, 378 (2d Cir, 1987), stated that "consent [is inherent] where a person's behavior manifests acquiescence or a comparable voluntary [act diminishing] his or her otherwise protected rights." See also Gantt, *supra* note 4, at 356-57, stating that "courts will imply consent when the employee knew or should have known of a policy of constantly monitoring calls or when the employee conducts a personal conversation over a line that is explicitly reserved for business purposes only." (Citing *Watkins v. LM Berry & Co.* 704 F.2d 577, 581-82 (11th Cir. 1983), and *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 396 (W.D. Okla. 1978), *aff'd.*, 611 F.2d 342 (10th Cir. 1979).)
33. *Id.*, Gantt, at 357-58. Citing *Jandak v. Village of Brookfield*, 520 F. Supp. 815 (N.D. Ill. 1981) where the court refused to find consent even though it found that a police officer should have known of an the interception of call since the police department routinely monitored calls; and *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992) where the employer had notified the employee only that "it might begin monitoring" the telephone calls.
34. Baumhart, *supra* note 4, at 395.
35. Gantt, at 357-58. Citing Baumhart, *Id.*; and Jennifer J. Griffin, "The Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee

Privacy Rights," 4 Software L.J. 493, 494 (1991). See also Hash and Ibrahim, *supra* note 4, at 900. "[M]onitoring business communications and the inadvertent monitoring of personal communications could be allowed if an employer has a written policy addressing E-mail monitoring. In such cases, employees using the system may be considered to have given consent." (Citing Watkins, 704 F.2d 577.)

36. Employees have an obligation to follow the rules and policies of their employers, and those who refuse to sign acknowledgment forms could be disciplined or discharged. At will employees may be terminated by an employer for any reason, or for no reason, unless the discharge clearly violates public policy. See *Smyth v. Pillsbury*, 914 F. Supp. 97, 99 (E.D. Penn. 1996) and *Roe v. Quality Transportation Services*, 67 Wash. App. 604, 607, 838 P.2d 128, 129 (Wash App.) 1992, discussing termination of at will employees.
37. *Id.*, Gantt, at 406. Gantt discusses the possibility that e-mail monitoring policies may increase tensions in the workplace generating resentment, suspicion and mistrust. Gantt also points out that e-mail provides an informal and beneficial conversational outlet for employees, and implies that a policy that is too restrictive may negatively impact efficiency and productivity.
38. Baumhart, *supra* note 4, at 394-95.

3. FEDERAL COURT DECISIONS ON MONITORING EMPLOYEE E-MAIL

Two federal court cases that specifically involve employer monitoring of employee E-mail have been reported. *Bohach v. The City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) addresses access to stored communications under the Electronic Communications Privacy Act of 1986 (ECPA) and the Fourth Amendment. *Smyth v. The Pillsbury Company*, 914 F. Supp. 97 (E.D. Penn. 1996) examines an employer's interception of employee E-mail as a tort action under Pennsylvania's common law. Although *Smyth* was decided under Pennsylvania law, it provides insight into a federal judge's reasoning concerning employer E-mail monitoring issues. Both courts conducted a balancing test of the employee's reasonable expectation of privacy and the employer's legitimate business interests.

The ECPA and the Fourth Amendment - Accessing Stored Information

Bohach v. The City of Reno is the only reported federal court decision addressing employer monitoring of employee E-mail under the ECPA. Plaintiffs, both Reno Police officers and subjects of an internal investigation, alleged that the Reno Police Department violated the ECPA and their constitutional right to privacy by accessing "Alphapage" electronic communications stored on the department's computer network.¹

Analyzing the facts under the ECPA, the court equated Alphapage communications to E-mail,² and stated that they were electronic communications, and not wire or oral communications, since they "did not involve the human voice." The court distinguished interception of a communication at the time of transmission from retrieval of the communication after it had been stored, and concluded that an electronic communication "by definition" could not be intercepted while in storage.³ The court found that the City of Reno was the "'provider'" of the "'electronic communications service,'" and under 18 U.S.C. 2701(c)(1), could "do as [it] wish[ed] when it [came] to accessing communications in electronic storage." Therefore, the court held that "neither [the city] nor its employees [could] be liable under 18 U.S.C. 2701."⁴

In the court's opinion, even if an intercept had occurred, "consent would likely be conferred under [18 U.S.C. 2511(2)] 'in light of the plaintiffs' decision to send those messages,... for one who sends a message using a computer must surely understand that the message will pass through the computer.'"⁵

Examining the Fourth Amendment privacy claim, the court reasoned that "at a minimum," plaintiffs had to "demonstrate that they had a reasonable expectation of privacy in their use of the Alphapage system."⁶ The court concluded that under the circumstances, their expectation was not objectively reasonable, and listed the following reasons why it felt that plaintiffs had only a "diminished expectation of privacy:" the police chief's notice and warning;⁷ the limited number of persons that could be contacted; the primary purpose of the system; and the "routine and proper practice" by police departments of "recording their communications with the public."⁸

Common Law Right to Privacy - Interception of Employee E-mail

In *Smyth v. The Pillsbury Company*, Smyth claimed that Pillsbury had wrongfully discharged him after intercepting his private E-mail messages. Pillsbury claimed the messages contained "inappropriate and unprofessional comments."⁹ The court assumed that all of the facts alleged by Smyth were true, and found that Pillsbury had not invaded his privacy by intercepting his e-mail.

Although Pillsbury's E-mail system was used to transmit "internal corporate communications," the company "repeatedly assured its employees, including Smyth, that all communications would remain confidential and privileged," and that "the E-mail communications could not be intercepted" and used against the employees to support disciplinary or discharge actions. Relying on the company's guarantee, Smyth responded to E-mail messages he had received from his supervisor, and the two exchanged E-mail over a period of time. Pillsbury intercepted the E-mail messages and discharged Smyth for the inappropriate content of the messages.¹⁰

The court examined whether Pillsbury's actions violated Smyth's right to privacy under Pennsylvania common law.¹¹ The court determined that the proper approach would be to "examine the facts and the circumstances surrounding the alleged invasion of privacy," and to balance "the employee's privacy interest against the employer's [legitimate business] interest."¹² In doing so, the court found that an employee does not have a reasonable expectation of privacy to e-mail communications he voluntarily makes over his employer's e-mail system, "notwithstanding any assurances" that the company would not intercept e-mail communications. The court noted that the e-mail system was "apparently used by the entire company," and said that Smyth lost any reasonable expectation of privacy once he transmitted his comments over the system to a second person.¹³ Additionally, the court stated that even if it had found that "an employee had an expectation of privacy in the contents of his E-mail," Pillsbury's interception of Smyth's e-mail was not a "substantial and highly offensive invasion of his privacy, an essential element in his cause of action. The court concluded that an employer's interest in preventing inappropriate and unprofessional conduct or even illegal activity over its [E]-mail system outweighs any privacy interest the employee may have in those comments."¹⁴

The courts in each of the above cases required that an employee demonstrate an objectively reasonable expectation of privacy in the contents of his or her e-mail messages. Each examined the circumstances surrounding the e-mail monitoring, and conducted a balancing test between the employee's reasonable privacy interests and the employer's legitimate business interests. Each court found that the employer's interest outweighed those of the employee. Although the Bohach court found that employees had at least a diminished expectation of privacy, the Smyth court found that an employee had no reasonable expectation of privacy and indicated that, at least under Pennsylvania law, an employer may monitor employee e-mail without an employee's consent. Nevertheless, it would be prudent for an employer to obtain employee consent to e-mail monitoring through a written e-mail policy. The Bohach court specifically cited the police department's notice and warning to Alphaspace users as a factor in diminishing the expectation of privacy, and alluded to consent as an exception to the ECPA's

prohibition on interception.

ENDNOTES
FEDERAL COURT DECISIONS ON MONITORING EMPLOYEE E-MAIL

1. Bohach v. The City of Reno, 932 F. Supp. 1232 (D. Nev. 1996). The police department had installed a software program called Alphapage on its Local Area Network (LAN) computer system to notify the media of news releases and other information over pagers that had been issued to between 40 and 70 members of the press. The program allowed short alphanumeric (non-voice) messages to be transmitted to a recipient's pager from any police department computer terminal. After logging on to the department's system and entering Alphapage, the sender selects a recipient from a list of persons to whom pagers have been issued, types the message, and "hits the send key." The message is processed through the computer system's Inforad Message Directory, and stored on a server file. The computer's modem dials the pager company's modem, sends the message, and disconnects. The pager company radio broadcasts the message to the recipient.
2. Id. The "phase at issue here (from the user's keyboard to the computer) is essentially electronic mail--and e-mail messages are, by definition, stored in a computer."
3. Id. The court noted the definition of electronic communication under 18 U.S.C. 2510(12) included transfer of signals and data, but did not include electronic storage, and specifically excluded it from wire (which includes both transfer and storage) and oral communication as defined under 18 U.S.C. 2510(1)(2) and (12). "An electronic communication may be put into electronic storage, but the storage is not itself the communication. Citing Jackson Games, Inc. v. United States Secret Service, 36 F. 3rd 457, 461-62 (5th Cir. 1994); and 18 U.S.C. 2701. In the court's opinion, since 18 U.S.C. 2510(4) defines intercept as the use of "any electronic, mechanical or other device" to acquire the "contents of any ... electronic ... communication," there could not have been an interception since "no computer or phone lines have been tapped, no conversations picked up by hidden microphones, no duplicate pager 'cloned' to tap into messages intended for another recipient." The court did not elaborate on its implication that a message is entitled to greater protection against contemporaneous recording (interception) during its transmission than against retrieval of stored communications (accessing archives made in the normal course of business).
4. Id.
5. Id. The Alphapage Media Notification System was installed on the police department's computer network by order of the police chief. "The order warned all users that 'every Alphapage message is logged on the network,' and prohibited some types of messages (e.g., those containing comment on Department policy, and those whose contents violated the Department's anti-discriminatory policy)."

6. Id. "We assume that they did indeed have a subjective expectation of privacy, if only because we cannot believe that, had they thought otherwise, they would have ever sent over the system the sorts of messages they did send." The court did note that "no special password or clearance was needed, and that Alphapage was accessible to any knowledgeable person with access to the police department's computer system."
7. Id. "[T]hat is not the same as saying that the content of all messages will be recorded and retained, but it suggests that one should expect less privacy on Alphapage than on, say a private telephone line." The court also noted that storage of communications was an "integral part of the technology, and "all [Alphapage] messages [were] recorded and stored not because anyone is 'tapping' the system, but simply because that's how the system works."
8. "[P]olice stations often record all outgoing and incoming phone calls for a 'variety of [legitimate] reasons,....' [f]or Fourth Amendment reasons, the point is that the practice is part of the 'ordinary course of business,' and it is all the more reasonable in this case in light of Alphapage's purpose and limitations." The court noted that the purpose of the system was to allow police personnel to communicate among themselves and with members of the press about "police matters;" and the fact that the system could be used by police personnel to transmit private communications was "incidental to its primary function."
9. *Smyth v. The Pillsbury Company*, 914 F. Supp. 97, 98-99, n1 (E.D. Penn. 1996). The messages referred to "sales management and contained threats to 'kill the backstabbing bastards' and referred to the planned Holiday party as the 'Jim Jones Koolaid affair'."
10. It is not clear from the facts presented by the court whether Pillsbury intercepted Smyth's messages during transmission or accessed them from storage. Since the court limited itself to applying common law rather than the ECPA, it may have felt that there was no need to make the distinction.
11. *Smyth*, supra note 9 at 100. Citing *Borse v. Piece Goods Shop, Inc.*, 963 F. 2d 611, 625 (3d Cir. 1992). The court concluded that in Pennsylvania, the particular "action for invasion of privacy is the tort of intrusion upon seclusion." The court that concluded that, in this case, the intrusion was not "substantial" and "highly offensive to the ordinary and reasonable person" as required by Restatement (Second) of Torts, section 625B. Most states recognize some type of common law invasion of privacy action. A federal court will analyze issues arising under state law as it believes a state court would under the circumstances, and the federal court must apply the substantive law of the particular state. Judicial interpretation of a particular statute, constitutional provision, or common law principle may vary from one federal jurisdiction to another and from state to state.
12. Id.

13. *Id.*, at 101.

14. *Id.* Smyth originally pled only wrongful discharge. He never claimed that Pillsbury had violated his rights under the ECPA. Finding that there was no action under Pennsylvania law for wrongful discharge of an at-will employee, the court supplied a possible invasion of privacy cause of action for Smyth under Pennsylvania common law, and then proceeded to explain why Smyth had failed to state a claim upon which relief could be granted. The court never made any reference to the ECPA or its exceptions.

4. THE FOURTH AMENDMENT E-MAIL MONITORING BY THE GOVERNMENT OR ITS AGENTS

An employer has a right and an obligation to investigate employee wrongdoing and protect its business and security interests. Federal, state and local government employers have the right to manage their employees to the same extent as a private employers do, including monitoring job-related conduct and conducting inquiries into job-related wrongdoing. A government employer generally may search its employees and their personal effects without a warrant to support administrative inquiries, disciplinary actions, or termination of employment for job-related misconduct. A government employee's legitimate expectation of privacy may be reduced by work place procedures, policies or requirements. The courts have recognized that government employers may search without a warrant an office or desk to which an employee has a reasonable expectation of privacy for documents which are lost, missing or needed to conduct government business.¹ Such a search must be "justified at its inception" and reasonable in its scope.²

To date there has been only one reported federal case that discusses e-mail monitoring by a government employer under the Fourth Amendment. The language of the Electronic Communications Privacy Act (ECPA) does not distinguish between private individuals, government entities, and individuals acting on behalf of the government,³ except that the ECPA does require the government, at least in criminal matters, to obtain a warrant or a court order prior to accessing stored information.⁴ Depending on the circumstances, e-mail monitoring by a government employer would have to conform to Fourth Amendment requirements, as well as to the provisions of the ECPA. Although private employers are not constrained by the Fourth Amendment, it may apply to a government contractor as an agent of the government for activities it conducts under the "direction of federal regulations or the direction of law enforcement authorities."⁵ Cases discussing Fourth Amendment invasion of privacy issues in the context of employers investigating employee conduct offer important insight into how the courts are likely to balance the employee's expectations against the

employer's interests in both government and private e-mail monitoring.⁶

Items or information found incidental to administrative searches without a warrant may be turned over to law enforcement authorities for prosecution and may be used as evidence in a criminal prosecution. The requirement is that the search must have been initiated and conducted by the government employer, or its agent, for its own legitimate business purposes, and not for the purpose of obtaining evidence for criminal prosecution.⁷ Evidence seized from an employee by a private employer acting alone and not as an agent of the government may generally be turned over to law enforcement authorities and used for criminal prosecution even though it has been wrongfully seized. However, a warrantless search conducted by a private employer under the authority of the government, at the suggestion of the government, or aided by the government for the purposes of criminal prosecution will likely result in the exclusion of the evidence under the Fourth Amendment.⁸

ENDNOTES
THE FOURTH AMENDMENT
E-MAIL MONITORING BY THE GOVERNMENT OR ITS AGENTS

1. O'Connor v. Ortega, 480 U.S. 709, 717 (1987). While affirming that a government employee may have a reasonable expectation of privacy in his or her workplace, the court noted that "operational realities" may sometimes make these expectations unreasonable. The court stated that a government employee's expectation, like the similar expectation of a private employee, "may be reduced by...actual office practices and procedures, or by legitimate regulation." See also Schowengerdt v. United States, 944 F2d. 483, 488-89. The court found that a civilian employee of the Navy "did not have a reasonable expectation of privacy to his office, his locked credenza," or in an envelope marked personal because he was "on notice from his employer" that security searches "might occur from time to time for work-related purposes." Adopting a balancing of the interests approach, the Ortega court articulated a "reasonableness under all the circumstances" Fourth Amendment test for a government employer's intrusions on the privacy interests of a government employee. The government's interest in the "efficient and proper operation of the workplace" justifies "work-related intrusions" by a government employer for "work related, non-investigatory reasons," as well as for "non-criminal investigations" into work-related misconduct. The court stated that government employees are often "entrusted with tremendous responsibility, and the consequences of their misconduct or incompetence to both the agency and the public interest can be severe." The court noted that government employees are provided with offices "for the sole purpose of facilitating the work of an agency," and an employee may "simply leave [personal belongings] at home" to avoid exposing them to intrusion by an employer. Ortega, at 723-725. See also Julia T. Baumhart, "The Employer's Right to Read Employee E-mail: Protecting Personal Property or Personal Prying?," 8 Lab. Law. 923, 939-943 (1988).
2. Id., at 726. A search is justified at its inception when a reasonable suspicion exists that the search will disclose evidence of work-related misconduct, or "that the search is necessary for a non-investigatory work-related purpose such as to retrieve a needed file." A search is limited in its scope "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct" [or the work-related need]. Citing New Jersey v. T.L.O., 469 U.S. 325, at 341-42.
3. See Larry O. Natt Gantt, II, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace," 8 Harv. J. Law and Tec. 345, at 352, n53 (1995). Citing 18 U.S.C. 2511(1)(a), (2)(a)(ii)(A).
4. Id., at 352, and n59 at 353. Citing 18 U.S.C. 2703(a)(b). Gantt also points out that a warrant is needed for communications stored on a communication service provider's system for 180 days or less, but may not be required for information stored more than 180 days if the government provides prior notice to the "subscriber or customer" and obtains an

administrative subpoena or a court order. If exigent circumstances exist, the government may be allowed to give delayed notice, or may be exempted from giving notice altogether.

5. *Id.*, at 380, n232. See also *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328 (9th Cir. 1987); 2 IER Cases 545, 550-52 (9th Cir. 1987). The court articulated two tests, either of which may be used to support government action or action under the color of law by a private party. Under the "public function test," government action exists where a private entity exercises "powers traditionally exclusively reserved for the state." (Citing *Jackson v. Metropolitan Edison, Co.*, 419 U.S. 345, 352 (1974)). Under the "joint action test," a private entity "is acting under the color of...law" if it "is a willful participant in joint action with the [government or its agents]." (Citing *Dennis v. Sparks* 449 U.S. 24, 27 (1980); and *Howerton v. Gabica*, 708 F.2d 380, 383, (9th Cir. 1983). The court stated that the "private status of a party may not be used to defeat a [constitutional violation claim] if the party engaged in federal action."
6. *Id.*, *Gantt*, at 380.
7. See *O'Connor*, at 725-26; *United States v. Blok*, 188 F2d. 1019 (CA DC 1951); *United States v. Bunkers*, 521 F2d 1217 (9th Cir 1975); *United States v. Collins*, 349 F.2d 863 (2nd Cir. 1965).
8. See *Burdeau v. McDowell*, 256 U.S. 465 (1921). Evidence seized by a private employer acting alone on its own behalf may be used as evidence in a subsequent prosecution.

5. E-MAIL MONITORING UNDER STATE LAW

This section discusses only e-mail monitoring and privacy issues under Washington law because the Pacific Northwest National Laboratory is located in Washington State.¹ Many states have enacted wiretap or eavesdropping statutes that are more restrictive than the Electronic Communications Privacy Act (ECPA). Some state statutes specifically address electronic communications while others do not; some provide an exemption only if there is consent of all parties to a communication; and some either specifically include or exclude employers.² Since privacy law and its judicial interpretation will vary among states, each national laboratory should become knowledgeable of the e-mail or electronic communications law of the particular state in which it is located, as well as the law of each state in which it maintains facilities and staff. Each laboratory should establish its own e-mail policy consistent with state and federal law and tailored to its particular workplace environment and security interests. Despite the differences in state laws, the common legislative intent and judicial purpose in all states is an attempt to balance the privacy interests of the individual against the legitimate interests of the employer.

Revised Code of Washington 9.73.030

The Revised Code of Washington (RCW) 9.73.030 covers "intercepting, recording [and] divulging private communications." The statute specifically applies to individuals, business entities, and government agencies; and prohibits interception or recording of private conversations and "private communication transmitted by telephone, telegraph, radio, or other device."³ Violation of the provisions of the statute is a gross misdemeanor,⁴ and the violator may be subject to a civil suit for monetary damages.⁵ Information acquired in violation of the statute may be inadmissible in any state court criminal or civil proceeding.⁶

The current statute does not specifically refer to e-mail or electronic communications, but in January 1996, House Bill 2766 was introduced in the Washington House of Representatives

that if passed, would amend RCW 9.73.030 to include e-mail. The bill specifically expresses the legislature's intent to address "privacy concerns" relating to "private" electronic communications, including e-mail. The bill also indicates a legislative intent to protect stored communications.⁷ Unfortunately, neither the statute nor the bill define terms such as "private communication", "private conversation", "electronic communications", "e-mail", "interception", or "stored communications".

RCW 9.73.030 contains an exception as long as prior consent is obtained from "all" the parties.⁸ It is unclear how the requirements of the consent exception would be applied to e-mail. It appears that implied consent may be sufficient as long as notice is given to all participants "in a reasonably effective manner" that the particular communication or conversation is about to be recorded. However, there is no explanation of what constitutes "reasonably effective" notice. If a private communication or conversation is recorded, the notice must also be recorded. It is not clear whether a published company e-mail monitoring policy would satisfy the requirement, or even whether a general on-screen notice at e-mail log-on would be sufficient. It may be that each e-mail message would have to contain a notice. Even so, unless the sender or recipient was a member of the company, he or she would not have received prior notice. It is also not clear whether e-mail storage would be considered a recording. It is interesting to note that in spite of the urgent need expressed by the legislature in the bill to address privacy issues, and its express intent to include e-mail, it made only minimal changes to the substantive language of the statute. Additionally, the legislature chose to make no changes to the consent provision. Because the proposed house bill was not passed during 1996 regular legislative session, it will have to be re-introduced during the next session. Therefore, an opportunity exists to work with the legislature to craft language that clarifies the issues identified above.

Judicial Interpretation of Current RCW 9.73.030

No Washington court cases were found that involved e-mail monitoring.⁹ However, there were

numerous cases applying RCW 9.73.030 to telephone monitoring by law enforcement agencies. Although the holdings in these cases are not relevant to the issues relating to employer monitoring of employee e-mail, several of the cases contain judicial interpretations of various terms used in the statute. In this limited regard, they provide some insight to how a court might apply RCW 9.73.030 to e-mail monitoring by employers.

Washington courts have noted that RCW 9.73.030 is more restrictive than the ECPA, and provides greater protection for the individual.¹⁰ However, the Washington statute only protects private communication and conversation, neither of which are defined in the statute.¹¹ If office e-mail is not considered private communication, the statute will not apply. Unfortunately, Washington courts have not yet decided a case in which the privacy of employee e-mail was at issue. In the cases involving telephone monitoring, the courts have held that "private conversation" is to be given its ordinary and usual meaning" considering the "intent or reasonable expectations of the participants as manifested by the facts and circumstances of each case."¹² This language indicates that, in an e-mail case, a Washington court would analyze the objective and subjective expectations of both the employer and the employee to determine reasonable expectation of privacy. A formal e-mail monitoring policy and effective notice to employees are important to an employer's position that office e-mail is not a communication to which its employees have a reasonable expectation of privacy, and therefore, not private communication under the RCW 9.73.030. The type and extent of notice necessary to sufficiently diminish an employee's expectation of privacy in his or her office e-mail under Washington law is uncertain, but it is likely that the courts would attempt to balance the employee's reasonable expectation of privacy against the employer's legitimate business interests as the federal courts have done.¹³ The courts may be reluctant to extend statutory protection to e-mail under a statute that protects oral and wire communications, but does not specifically include e-mail or electronic communications. One commentator suggests that California state court decisions on employee privacy claims might be used as a guide by other state courts because California has a "well developed" private employment privacy standard.¹⁴ California courts have decided several e-mail privacy suits in favor of employers based on lack

of employee expectation of privacy, and because the wiretap statute did not encompass e-mail.¹⁵

Common Law Invasion of Privacy

Washington and many other states recognize a common law action for invasion of privacy which employees may use as an alternative to statutory law. Although there are several possible causes of action under invasion of privacy, intrusion upon seclusion is one of the most likely to be claimed by an employee against an employer that monitors e-mail.¹⁶ The "interference with a plaintiff's seclusion must be a substantial one resulting from conduct of a kind that would be offensive and objectionable to the ordinary person."¹⁷ Although no Washington invasion of privacy decisions relating to employee e-mail were found, the "substantially offensive and objectionable" standard is the same one used by the court in *Smyth v. Pillsbury Company* when it found that a "reasonable person" would not have considered Pillsbury's interception of Smyth's e-mail to be a "substantial and highly offensive invasion of [his] privacy."¹⁸ A California court rejected the invasion of privacy claims of two employees who were fired after they complained to their employer about its monitoring of their personal e-mail messages. The court held that they had no reasonable expectation of privacy in their e-mail because they had signed a user form acknowledging that it was company policy that use of company-owned computer hardware and software was restricted to company business. Additionally, the employees admitted that they had known that their messages were being monitored for months before they were discharged.¹⁹

Constitutional Law

Washington courts have held that the state "has a long history of extending strong protections to telephonic and other electronic communications,"²⁰ and that Article 1, Section 7, of the Constitution of the State of Washington "creates a right to privacy"²¹ that "expressly" protects a person's "private affairs."²² However, unlike the California constitution's privacy provision,

which the California courts have applied to private business "as well as government activities," the Washington constitutional provision has been interpreted as applying only to government action and not to individuals or entities acting in a private capacity.²³ Given the Washington courts' explicit recognition that Article 1, Section 7, provides greater protection for the individual against government intrusion than the Fourth Amendment of the U.S. Constitution, one would expect that, in an e-mail case in which there was a constitutional privacy issue, a court would give significant weight to factors supporting an employee's reasonable expectation of privacy, but a court would also consider the competing legitimate interests of the employer.²⁴

Summary

It is unclear how the Washington courts would apply RCW 9.73.030 to e-mail at this time since the language does not include the terms "e-mail" or "electronic communication." If House Bill 2766 is re-introduced, and the legislature ultimately adopts the text of the original bill, the statute will clearly encompass e-mail. Even so, it still may not be clear whether office e-mail is the type of communication that can reasonably be construed as private communication, especially if a clear company e-mail policy has been published in a manner designed to give reasonable notice to employees. A common law action for invasion of privacy would have to demonstrate substantial and highly offensive intrusion. Nevertheless, the Washington legislature and the courts have expressly emphasized the importance of privacy concerns. The courts can be expected to apply a balancing of the interests analysis in evaluating all types of privacy claims. Any employer who monitors employee e-mail should ensure that monitoring is conducted in the normal course of business for legitimate business reasons. This is especially important for government employers whose actions may have to survive constitutional scrutiny.

ENDNOTES
E-MAIL MONITORING UNDER STATE LAW

1. Statutes and court decisions from other states are cited for illustrative purposes.
2. See Generally, Paul E. Hash and Christina M. Ibrahim, "Selected Topics on Employment & Labor Law: E-Mail, Electronic Monitoring, and Employee Privacy", 37 S. Tex. L. Rev. 893, 904-05 (1996); Larry O. Natt Gantt, II, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace", 8 Harv. J. Law and Tec. 345, 395-403 (1995); and Laurie Thomas Lee, "Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop'," 28 J. Marshall L. Rev. 139, 158-60 (1994), discussing the application of state statutes to electronic communication and employee privacy issues. Idaho and New Mexico are among the states that have statutes with prior consent and business use exemptions, and Nebraska's wiretap statute specifically exempts employers. (Hash and Ibrahim, at 905, n81; Gantt, at 402). Washington, Illinois, and California are examples of states that require the consent of all the parties to the communication. (Gantt, at 395, n332). Connecticut prohibits electronic surveillance of employees in areas such as restrooms, lounges, rest and recreation areas, and locker rooms; prior notification is not an exception. Nevada prohibits "surreptitious monitoring of private conversations." Neither state's statutes specifically apply to e-mail or computer files (Gantt, at 401, n380; and Lee, at 160 n.118).
3. RCW 9.73.030(1). "Except as otherwise provided in this chapter, it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any: (a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication; (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all persons engaged in the conversation."
4. RCW 9.73.080.
5. RCW 9.73.60. Either actual damages or liquidated damages of \$100.00 per day, not to exceed \$1000.00, plus reasonable attorney's fee's and costs, are available for injuries to person, business or reputation resulting from a violation of RCW 9.73.030.
6. RCW 9.73.050.
7. The bill was introduced on January 18, 1996 and referred to the House Committee on Law and Justice. H.B. 2766, 54th Legis., Reg. Sess. (1996). "[NEW SECTION] Sec. 1.

The legislature finds the use of electronic means of communications such as **electronic mail** and facsimiles has outpaced, and poses new challenges for, laws and regulations governing privacy. Specifically, the legislature finds that while state and federal laws prohibit the interception or recording of private communications, including those by electronic means, it is unclear whether any law protects the privacy of **stored** electronic communications. The legislature further finds that as the use of electronic technology has increased dramatically in governmental, business, and personal communications, the **need to address privacy concerns has become increasingly urgent**. Sec. 2(1) Except as otherwise provided in this chapter, it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, **[read, alter,]** or record any: (a) Private communication transmitted by telephone, telegraph, radio, **[electronic mail, facsimile,]** or other device....” (Emphasis added to highlight new text. The rest of the language of the bill is the same as the current provision.)

8. RCW 9.73.030(3). “Where consent by all parties is needed pursuant to this chapter, consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded.”
9. Gantt, *supra* note 2, at 379, n221. Gantt cites Washington Fed’n of State Employees v. Department of Labor and Indus., No. 90 2 02130 8 (Wash. Super. Ct. filed Sept. 10, 1990) as an e-mail privacy case involving public employees, but it was apparently unreported.
10. State v. Goucher, 124 Wash. 2d 778, 785, 881 P. 2d 210 (1994). (Citing State v. Gunwall 106 Wash. 2d 54, 66, 720 P. 2d 808 (1986) and State v. O’Neill, 103 Wash. 2d 853, 861-67, 700 P. 2d 711 (1985)). “Washington’s privacy act is one of the most restrictive in the nation.” State v. Faford, 128 Wash. 2d 476, 481, 910 P.2d 447 (1996). (Citing O’Neill, at 878). The ECPA does not preempt RCW 9.73.030. State laws may be more restrictive than federal laws, and unless there is conflict of law, the state statute may be applied instead of the federal statute. See State v. Williams, 94 Wash. 2d. 531, 539, 617 P.2d 1012 (1980). (Applying the state statute to suppress the interception and recording of private telephone conversations by federal agents that complied with the ECPA, but violated the provisions of RCW 9.73.030.). See also Lee, *supra* note 2, at 158, n104.
11. State v. D.J.W., 76 Wash. App. 135, 140, 882 P. 2d 1199 (1994). Affirming that RCW 9.73.030 applies to both private and state governmental agencies, but protects only private conversation and communication.

12. *Id.*, at 140-41. The court defined private as “‘belonging to one’s self...secret...intended only for the persons involved (a conversation)...holding a confidential relationship to something...a secret message: a private communication...secretly: not open or in public. (Citing *State v. Forrester*, 21 Wash. App. 855, 861, 587 P.2d 170 (1978), review denied 92 Wash. 2d 1006 (1979), quoting from Webster’s Third New International Dictionary (1969). See also *State v. Faford*, supra note 10, at 484-86. The court used this expectation of the parties approach and found that the defendant had reasonable expectation of privacy to his cordless phone conversations which were intercepted by his neighbor’s scanner, the information from which led to a warrantless police search. While the court did not “deny the relevance of objective factors” determine privacy, it focused on the subjective expectations of the parties. Absent a showing that the defendant’s phone or owner’s manual bore any privacy warning, the court refused to allow the prosecution to submit evidence that owner’s manuals for five commercially available cordless phones contained warnings about the possibility of interception of phone calls. In finding that the term “transmit” should be defined broadly, the court found that the scanner was a “device ... designed to record or transmit ...” as contemplated by the statute. The court stated that the fact that “the mere possibility of intrusion on otherwise private activities is technologically feasible will not strip citizens of their privacy rights,” and that it would “not permit the introduction of new communications technology to defeat the traditional expectation of privacy in telephone conversations.” See also *State v. Slemmer*, 48 Wash. App. 48, 52-3, 738 P.2d 281 (1987). Considering the “intent or reasonable expectations of the participants” under the circumstances, the court found that an admission of wrongdoing that was surreptitiously recorded at an investment group meeting was not a private communication because the speaker knew that minutes were being kept and all participants knew that the substance of the meeting was available to the public. The speaker had no expectation of privacy in the communication between himself and the other group members during the meeting.
13. See *Bohach v. The City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996).
14. Julia T. Baumhart, “The Employer’s Right to Read Employee E-mail: Protecting Property or Personal Prying?” 8 Lab. Law 923, 944 (1992).
15. See Hash and Ibrahim, supra note 2, at 906-7; Gantt, supra note 2, at 359-60 and 398-401; and Lee, supra note 2, at 142 and 166-7. (Citing *Shoars v. Epson America, Inc.*, SWC112749, slip op. (D.C. Cal. 1990), No. B073243 (Cal. Ct. App.) review denied, No. SO40065, 1994; and *Flanagan v. Epson America, Inc.*, No. B073243, (Cal. Ct. Super. Ct. 1991)). Shoars, an Epson employee, provided e-mail training and support for other Epson employees. She had been told that employee e-mail was private, and had been told to provide that information to other Epson employees. Shoars discovered that her supervisor was routinely reading employee e-mail messages. Shoars was fired after she complained about her supervisor reading employee e-mail. She sued for wrongful termination. Shoars also joined other employees in a class action suit (*Flanagan v. Epson*)

for invasion of privacy. Both suits were dismissed. The Shoars court summarily found that Epson's conduct had not violated California Penal Code, Section 631 (a wiretap statute similar to Washington's current RCW 9.73.030). The Flanagan court found that expectation of privacy was an essential element of invasion of privacy, and it was not clear that employees had such an expectation to their e-mail. The court seemed to ignore Epson's assurances that employee e-mail was private. Furthermore, the court found that, even if employees had, an expectation of privacy, e-mail was not covered under Section 63, and that extending the provision to cover e-mail was the province of the legislature. In dictum the court implied that the provider exception of the ECPA would have exempted Epson from liability. The court stated that "there is simply no ECPA violation if 'the person or entity providing a wire or electronic communications service' intentionally examines everything on the system." (Quoting Ruel Torres Hernandez, "ECPA and Online Computer Privacy, 41 Fed. Com. L.J. 17 (1988), at 39).

16. *Eastwood v. Cascade Broadcasting Company*, 42 Wash. App. 88, 91-3; 708 P. 2d 1216 (1985). The court noted that "[a]lthough invasion of privacy... has received little attention in Washington, it is a recognized cause of action." The court noted that any of the four following interests, which are distinct from one another, may be involved under invasion of privacy: intrusion upon seclusion or solitude; public disclosure of private facts; publicly placing a person in false light; and appropriation of a person's name or likeness for personal advantage. (citing Prosser, "Privacy," 48 Calif. L. Rev. 383, 389 (1960).
17. *Id.*, at 92. (citing *Mark v. Seattle Times*, 96 Wash. 2d 473, 497, 635 P. 2d 1081 (1981), citing Restatement (Second) of Torts.
18. *Smyth v. The Pillsbury Company*, 914 F. Supp. 97, 100-01 (E.D. Penn. 1996). (Citing Restatement (Second) of Torts, Section 652B.) See a discussion of the case in the federal court section of this paper.
19. Hash and Ibrahim, *supra* note 2, at 907; and Gantt *supra* note 2, at 378-79. (Citing *Bourke v. Nissan Motor Co.*, YC003979 (Sup. Ct. Cal. 1991), No. B068705 (Ca. Ct. App. 1993). The messages sent by the two employees contained inappropriate jokes and language, some of which was sexually oriented. The employees had been hired to set up and run an e-mail system between dealers. Nissan warned the two employees about the content of their messages, and fired them after they complained about the monitoring. The court refused to find that the employees had an objective expectation of privacy merely because they had been issued passwords and told to protect them. See also Gantt, at 379. Citing *Washington Fed'n of State Employees v. Department of Labor & Indus.*, No. 902021308 (Wash. Super. Ct., filed Sept. 10, 1990) as an e-mail privacy case involving public employees and state action.
20. *State v. Gunwall*, 106 Wash.2d 54, 66, 720 P. 2d 808 (1986). This was a case involving access by the state, without a warrant, to long distance phone records and the use of a pen register to obtain locally dialed phone numbers.

21. *Roe v. Quality Transportation Services*, 67 Wash. App. 604, 608, 838 P. 2d 128 (1992). Roe was fired for refusing to submit to random drug testing. She claimed wrongful discharge and invasion of privacy. In addition to finding that "there is no authority in [the State of Washington] for applying ... constitutional restraints to private citizens," the court failed to find a "mandate of public policy" in either RCW 9.73 or in common law to preclude mandatory drug testing by a private employer.
22. *Gunwall*, *supra* note 19, at 65.
23. *Roe*, *supra* note 20, at 608.
24. *Id.*, at 610. The court suggested that a consideration of the "competing interests of the private employer and the employee" was the appropriate approach to applying statutory and common law as well as constitutional law, but indicated that, at least in statutory matters, it would look to the legislative intent since the "legislative process ... was uniquely suited to...defining and balancing the employee's privacy interests and the employer's interests...."

6. E-MAIL MONITORING POLICY AND NOTICE CONSIDERATIONS

Current legislation and jurisprudence is just beginning to grapple with the parameters of E-mail monitoring by employers.¹ Most commentators agree that until these boundaries are more clearly defined, an employer who wants to reduce its potential liability should establish a "well-drafted" and "clearly-defined" company e-mail policy that is communicated to its employees. These policies must define the company's rights, inform employees that e-mail is for business purposes only, warn employees that the employer monitors e-mail for business purposes, and advise employees that the employer can access any message at any time.² PNNL should ensure that employees are aware of the types of information that are considered trade secrets and proprietary. PNNL should also inform employees about the requirements for protecting ECI. Employees should be advised that e-mail is being monitored as part of PNNL's information protection program.

A company e-mail policy may be established as a separate policy or as part of a company's general electronic communication policy which includes computer and telephone use. In any event, a company's policy should be tailored to its particular security needs and workplace environment. The policy should accommodate, as much as possible, the needs of both the employer and the employees. An overly restrictive policy will undoubtedly result in morale problems and, if contested, may not be considered reasonable by the courts.³ In order to minimize the risk of civil or criminal penalties, e-mail monitoring policy should be consistent with federal and state laws.⁴ An objective, well-defined company policy that is communicated to the employees will allow an employer to demonstrate, if need be, that an employee had consented to the e-mail monitoring, or had a reduced expectation of privacy. Such an e-mail policy will also reduce an employer's potential liability for employee claims of discrimination and harassment, and will allow an employer to discipline or discharge an employee, if necessary, for violating company policy.⁵ However, once a company institutes a policy, it is bound by it, and may expose itself to liability if it exceeds the parameters set by its own policy. As with other company policies, an employer may change its e-mail policy without

exposing itself to additional liability as long as it gives appropriate notice to its employees.

One commentator has suggested the following guidelines for an effective e-mail policy:⁶

- Clearly communicate to employees that the security of E-mail...communications is not guaranteed. The policy should inform employees that the employer may override individual passwords and codes, and require employees to disclose all passwords and codes to the employer to facilitate such access (if requested).⁷
- Explain the employer's monitoring procedures and how they may be used by management.
- Provide for limited, authorized access to E-mail...communications, defining the scope of authorization.
- Provide that electronic...communications, including E-mail...communications and the contents of an employee's computer, are the sole property of the employer.
- Identify the reasons for surveillance and the specific business purposes to be achieved, such as [protecting trade secrets, proprietary information, or ECI], preventing excessive personal use of the company's systems, monitoring employees' service and effectiveness with clients and customers, assuring compliance with company policies, and investigating conduct or behavior that may be illegal or adversely affect the employer or the welfare of its employees.
- Provide that by using the employer's E-mail ... system and other equipment, including company computers, the employee knowingly and voluntarily consents to being monitored, and acknowledges the employer's right to conduct such monitoring. It [may] also be advisable to obtain from each employee a signed acknowledgment form memorializing the employee's consent to such monitoring,⁸ [or to emphasize that use of the e-mail system constitutes consent to monitoring by displaying an electronic message each time an employee logs on to e-mail, and requiring the employee use a PIN number after the message in order to actually activate his or her e-mail.]
- Prohibit the use of the employer's E-mail...system for personal messages, solicitation of employees, or distribution of information that is not related to the employer's business, with the exception of short informational messages or information posted on a designated computer "bulletin board."⁹
- [Provide that] communications [shall be consistent with company policy against] ... verbal abuse, slander, defamation, or trade disparagement of employees, customers, clients, vendors, competitors, or any other person or entity.

- [Provide that communications will conform to company policy against harrasing, threatening, or otherwise disparaging] others based on race, national origin, marital status, sex, sexual orientation, age, disability, pregnancy, religious or political beliefs, or any other characteristic protected under federal, state, or local law.¹⁰
- Prohibit employees from creating, distributing, or soliciting sexually-oriented messages or images, unwelcome sexual advances, requests for sexual favors, or other unwelcome conduct of a sexual nature.
- [Provide that employees will adhere to company policies concerning disseminating] or printing of copyrighted materials, including articles and software, in violation of copyright laws.
- Prohibit the [unauthorized] exchange of trade secrets, proprietary information, or any other confidential information via E-mail. Communications that may be [proprietary or] privileged (that is, communications to in-house counsel that may be subject to the attorney-client privilege) should be clearly identified as such, and encrypted for transmission.
- Prohibit employees from accessing or attempting to access the E-mail...system of another user or transmitting messages from a coworker's E-mail...system [without management approval].
- Explain the significance of the "Delete" and "Wastebasket" functions, and describe procedures for ensuring the permanent destruction of E-mail...communications (when desired).
- Inform employees regarding the potential discovery of stored E-mail...communications, including the use of such messages for litigation against the company. Simply by promoting this understanding, employers may encourage the cautious and appropriate use of E-mail and Voicemail systems.¹¹

ENDNOTES
E-MAIL MONITORING POLICY AND NOTICE CONSIDERATIONS

1. Donald H. Seifman and Craig W. Trepanier, "E-mail and Voicemail Systems. Evolution of the Paperless Office: Legal Issues Arising out of Technology in the Workplace, Part 1," 21 Employee Relations L. J. 3, page 5 (1995).
2. Seifman and Trepanier, *supra* note 1; and Larry O. Natt Gantt, II, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace," 8 Harv. J. Law and Tec. 345, 404-05 (1995).
3. Laurie Thomas Lee, "Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop,'" 28 J. Marshall L. Rev. 139, 173 (1994).
4. Gantt, *supra* note 2, at 405.
5. Seifman and Trepanier, *supra* note 1.
6. *Id.* The policy guidelines proposed by Seifman and Trepanier articulate the recommendations of most commentators who uniformly advocate a published company e-mail policy as the most effective means for an employer to reduce its risk of liability against employee privacy claims relating to e-mail monitoring. See also Gantt, *supra* note 2, at 404-408; Thomas, *supra* note 3, at 172-74; Paul E. Hash and Christina M. Ibrahim, "Selected Topics on Employment & Labor Law: E-Mail, Electronic Monitoring, and Employee Privacy," 37 S. Tex. L. Rev. 893, 909-10 (1996); and Thomas R. Greenberg, "E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute," 44 Am. U. L. Rev. 219, 249-50.
7. An employee's belief that passwords are completely personal, even if mistaken, may create a reasonable expectation of privacy. See Thomas, *supra* note 3, at 164, who states that the courts may consider a password to be equivalent to a "padlock on a locker." See Gantt, *supra* note 2, at 376, 379 and 382. Gantt states that a password creates at least a subjective expectation that e-mail messages are private, and this expectation may be "greater with systems that allow employees to create and modify personal passwords." However, notice to employees that the employer can nevertheless monitor e-mail messages will reduce or eliminate the employee's subjective expectation of privacy, and employee use after notification may be interpreted by the courts as implied consent. See also Ruel Torres Hernandez, "ECPA and Online Computer Privacy," 41 Fed. Com. L.J. 17, 31 (1988), stating that a password is an indication of privacy that may trigger "ECPA coverage unless the user has been notified to the contrary."

8. Amy Thompson and Sherry Harowitz, "Taking A Reading on E-mail Policy," *Security Management*, at 58, November 1996. United Airlines has a two phase employee awareness program: At new hire orientation, employees are given a security briefing, and must sign an e-mail policy acknowledgment, "verifying that they have read and understood it." Employees must renew their acknowledgment on a yearly basis by signing a statement "about security in general" that contains a sentence about e-mail security comprehension and compliance. See also Perkins Coie, "E-Mail: Even the Rose of Communication Has Some Thorns", 2 Wash. Empl. Letter 3, at 2.
9. *Id.*, Thompson and Harowitz, at 57. United Airlines employees must sign a form acknowledging that e-mail is for business use only. United periodically monitors e-mail to check on compliance, but does not strictly enforce "minor infractions, such as innocuous personal chit-chat between staff." *Id.*, Coie, at 2.
10. Seifman and Trepanier, *supra* note 1. Racially or sexually offensive communications (or offensive communications directed at age or disabilities) over e-mail systems could expose an employer to liability for allowing workplace harassment or discrimination. If an employer with the ability to detect communication containing inappropriate content fails to monitor e-mail, a court could conclude that a "'reasonable' employer would have conducted monitoring, and...may infer that the employer was aware of employees' pervasive inappropriate use of the E-mail..." These types of communications create hostile work environments that interfere with performance and are intimidating to many employees. See also Coie, *supra* note 8, at 2-3.
11. *Id.*, Seifman and Trepanier. Courts have held that e-mail and other electronic communications are discoverable, and employers may be compelled to produce them. Seifman reports that a court will "freely admit" e-mail messages into evidence and that they can be very damaging because they are written informally and the contents are often less inhibited than a written memorandum would be. *Id.*, Coie, at 2.

DISTRIBUTION

No. of
Copies

No. of
copies

OFFSITE

ONSITE

2 DOE/Office of Scientific and Technical
Information

1 DOE Richland Operations Office

T. Dedik

R. B. Goranson

K8-50

Nuclear Transfer & Supplier Policy
Division U.S. Department of Energy
Forrestal Building, GA-044
1000 Independence Avenue, SW
Washington, D.C. 20585

27 Pacific Northwest National Laboratory

Z. Hollander

R. E. Allen

K7-62

Nuclear Transfer & Supplier Policy
Division U.S. Department of Energy
Forrestal Building, GA-044
1000 Independence Avenue, SW
Washington, D.C. 20585

E. L. Benjamin (10)

K8-41

D. J. Bradley

K8-41

W. C. Cliff

K6-48

J. L. Fuller

K6-48

J. O. Heaberlin

K8-41

K. J. Krisher

K1-06

J. A. Nelson

K6-48

D. L. Nousen

K6-44

A. C. Rither

K1-67

M. A. Segura

K8-58

D. A. Varley

K1-06

C. E. Willingham, Jr.

K8-41

Technical Report Files (5)

C. Reindeau

Nuclear Transfer & Supplier Policy
Division U.S. Department of Energy
Forrestal Building, GA-044
1000 Independence Avenue, SW
Washington, D.C. 20585

A. Welihozkiy

Nuclear Transfer & Supplier Policy
Division U.S. Department of Energy
Forrestal Building, GA-044
1000 Independence Avenue, SW
Washington, D.C. 20585