E-mail privacy rights in business 18539 flashcard

E-Mail Privacy Rights In Business

E-Mail Privacy Rights in Business

I. Abstract

How far we have come in such a small time. When you think that the personal computer was invented in the early 1980’s and by the end of the millennium, several households have two PC’s, it is an astonishing growth rate. And, when you consider business, I can look around the office and see that a lot of the cubicles contain more than one PC. It is astonishing to me that such an item has taken control over the information technology arena like personal computers. Consider, however, the items that go along with personal computers: printers; modems; telephone lines for your modem; scanners; the software; online access; and lets not forget, e-mail addresses.

E-mail, or electronic messaging, has taken over the communications world as the preferred method of exchanging information. From the simple, “ let’s do lunch” messages, to the ability to send a business associate anywhere in the world an e-mail with an attached document that contains 150 megabytes of information, e-mail is quickly replacing the telephone, the U. S. post-office, and even overnight delivery services as primary method of exchanging important data.

With the ability to create and send this instant information, the technology has far outpaced the education of how to use this phenomena, the affects of this technology on society, and how to prevent this method of

communication from growing itself out of existence. Consider the following numbers:

· There were about 23 million e-mail users in 1994

· There will be approximately 74 millions e-mail users in the year 2000

· Employees sent approximately 263 billion e-mail messages in 1994

· Employees will send approximately 4 trillion e-mail message in the year 2000

· A 1993 study by MacWorld magazine found that 22% of employers have engaged in searches of employer computer files, voice mail, electronic mail, or other network communications

· The number of people subject to electronic surveillance at work has increased from approximately 8 million in 1990 to more than 20 million in 1996.

· Nearly 60% of companies that monitor e-mail or other employee communications conceal doing so.

· Less than 20% of companies have a written policy on electronic monitoring.

One of the major areas affected by this new technology is corporate America. Not only is it struggling with how to keep pace with the growing need for fast and efficient e-mail, but also the dangers associated with it. Among these dangers is privacy, in particular, what legal rights corporations and employees have in keeping their communications private. This paper will

introduce the current legislation in this area, the expectation of privacy an employee should have, any court decisions that provide additional ruling, and what a corporation can do to prevent litigation in these matters.

II. Employees Expectation of Privacy in e-mail

As an e-mail systems manager, I was under the impression that since the company owns the electronic messaging system, the company could view the contents of any employees e-mail account at any time. I was only partially right. The explanation of the current law will describe this in detail, but, the employee does have a certain right to privacy where e-mail is concerned.

Arguably, a company’s most valuable asset is it’s data. In the age of technological marvels, it is easier to create more valuable data and, on the other hand, that data is more easily retrievable, especially by persons not authorized to obtain the data. Employees of companies can expect a certain right of privacy granted by three main sources: (1) The United States Constitution; (2) Federal Statutes (The Electronic Communications Privacy Act of 1986); and (3) State Statutes (many of which have not addressed the issue).

The United States Constitution provides a limited group of employees with privacy safeguards. The safeguards are based on guarantees in the United States Constitution’s Fourth amendment and similar state constitutions. Courts have upheld that the Fourth Amendment’s protection against “ unreasonable search and seizures” applies to workplace invasions of privacy. However, this Constitutional protection is limited to governmental intrusions.

Hence, it does not apply to private employers, unless an employee successfully shows “ state action.” In Schowengerdt v. General Dynamics Corporation [823 F. 2d 1328, 1332 n. 3 (9th Cir. 1987).] Schowengerdt held that the employee had a reasonable expectation to privacy in work areas of exclusive use to the employee, such as the employee’s office, unless the employer had previously notified the employee that the employee’s office was subject to a work-related search on a regular basis. The court concluded that despite the employee’s reasonable expectation to privacy in his office that a warrantless search of the office was permissible when it was work-related and reasonable under the circumstances. As the wording of the 4th amendment suggests. it does not protect against all searches, only unreasonable searches. Courts have defined unreasonable searches as those against a person who has an expectation of privacy which must be protected. This can be shown in United States v. Perkins. [383 F. Supp. 922, 927 (N. D. Ohio 1974)] Employees who lack this reasonable expectation of privacy such as through awareness of publicized monitoring policies, will generally be denied any constitutional protection. The policy, to be effective, should warn employees that e-mail messages may be audited despite certain system features that give the appearance of privacy, such as personal passwords and the employee’s ability to delete messages.

III. Current Law Pertaining to E-mail Communication

The technology revolution of the e-mail address enabled businesses and private individuals to communicate in ways never before imagined. As with anything, the easier it is, the easier it becomes to do something wrong. With e-mail, this is very evident. In order to prevent wrongdoing and to protect

the e-mail user, Congress enacted the Electronic Communications Privacy Act of 1986 (EPCA). [Pub. L. No. 99-508, 100 Stat. 1848 (1986)(codified at 18 U. S. C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988)).] The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, [18 U. S. C. §§ 2510-2520 (1994).]. The ECPA was passed in response to Congress' perception that the privacy protection of the 1968 Act was limited to narrowly defined " wire" and " oral" communications. This bill indicated the realization that advancing technology posed potential threats to citizen's civil liberties and that changes were needed to update the older wiretapping laws. The amendment expanded the scope of Title III to include the interception of " electronic communication" and unauthorized access of stored electronic communications. [18 U. S. C. § 2510(1), (4), (12), (17) (1994).] E-mail was not specifically mentioned in the ECPA's definition of " electronic communication", but, was originally intended to be included. " Electronic communication" is defined as in the ECPA as the " transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. [18 U. S. C. § 2510(12)(1994). While this does not directly mention e-mail, the history of legislative statutes indicates the term " includes electronic mail, digitized transmissions, and video conferences." [S. Rep. No. 99-541, at 14 (1986)].

The ECPA also outlaws the interception of electronic communications. [18 U. S. C. §§ 2511(1)(a), 2520 (1994).] The ECPA amended the Federal Wiretap Act's definition of " intercept" as " the aural or other aquisition of the

contents of any wire, electronic, or oral communication.” [18 U. S. C. § 2510(4) (1994).] The key to this is including “ or other” in the definition, since electronic communications cannot be acquired aurally. Even though electronic communications are now included within the ECPA’s interception clause, the range of protection afforded by the prohibition against interception has been narrowly interpreted by one of the few courts to address the issue.

An example of this lies in the decision of the 5th Circuit Court in the case of Steve Jackson Games, Inc. v. United States Secret Service, [36 F. 3d 457 (5th Cir. 1994).] In this case, the court decided whether or not the Secret Service’s seizure of a computer that was used to operate an electronic bulletin board system, constituted an “ intercept” of the stored but unread e-mail contained on the system. Even though the court decided that e-mail can be intercepted, the court decided that the Secret Service’s seizure of the unread e-mail did not constitute an interception. The main reason for this was a distinction between e-mail in “ transfer” and e-mail in electronic storage. The use of the word “ transfer” in the definition of “ electronic communication,” and its omission in that definition of the phrase “ any electronic storage of such communication” says that Congress did not intend for “ intercept” to apply to “ electronic communications” when those communications are in “ electronic storage.” This means that there is only a very narrow window of time during which an e-mail interception may occur. This would be the time between the time an e-mail message is sent and the time it is saved to any location designated as storage. So, for all intents-and-

purposes, interception of e-mail within the prohibition of the ECPA is virtually impossible.

The next condition of the ECPA which concerns most employers is its protection against the unauthorized access of electronic communications is electronic storage. [18 U. S. C. § 2701 (1994).] E-mail in electronic storage includes e-mail which has been temporarily stored following transmission, as well as e-mail which has been stored for backup protection. [18 U. S. C. § 2510(17) (1994).] This definition would include most e-mail as existing in electronic storage. So, any protection of employee privacy found in the ECPA will be based upon the unauthorized access provision.

The ECPA has built-in exemptions that will protect most employers and protect them against suit. These exemptions are: prior consent, business use, and system provider.

1. Prior Consent

The best protection against liability under the ECPA is when prior consent has been given for any interception or access of e-mail in electronic storage. Interception of electronic communication is expressly allowed by the ECPA when “ one of the parties to the communication has given prior consent.” [18 U. S. C. § 2511(2)(d) (1994).] Also, access to stored electronic communication is allowed without liability when authorization has been given “ by a user of that service with respect to a communication of or intended for that user.” [18 U. S. C. § 2701(c)(2) (1994).] An easy case to understand here is American Computer Trust Leasing v. Jack Farrell Implement Co. [763 F. Supp. 1473, 1495 (D. Minn. 1991)]. Summary judgement was granted in this

case stating that when the party consented to the access of its computer system, it “ cannot now claim that such access was unauthorized.”

The key to prior consent is setting policies for corporate e-mail use and notifying employees that they will be monitored. This policy should be corporate-wide and employees that use the system will be judged as giving implied consent upon reviewing the policies and agreeing to the fact that they have read and reviewed the policies. Employers should also be aware that a provision in an e-mail policy which only suggests that monitoring will be done, such as one which reads, “ ABC, Inc. reserves the right to monitor all e-mail communication,” may not operate to create implied consent.

2. Business Use Exemption

Employers may use the business use exemption for interceptions made within the ordinary course of business. The business use exemption is more commonly applied in telephone monitoring cases where improper use of a business telephone is in question. Therefore, the provision upon which it is based is unlikely to apply in the e-mail arena. The definition of “ intercept” in the ECPA excludes interceptions captured by “ telephone or telegraph instrument, equipment, or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication services…being used by the subscriber or user in the ordinary course of business.” [18 U. S. C. § 2510(5)(a)(i) (1994).] Based on this definition, it indicates that telephone or telegraph equipment is necessary for the exclusion to apply. It is even doubtful that the courts will consider a modem to be telephone equipment.

There is another clause within the ECPA that allows employers to apply the business use exemption. Section 2511(2)(a)(i) states:

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 of electronic communication service, whose facilities are used in the transmission of a wire of electronic communication, to intercept, disclose, or use that communication in the normal course of 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. [18 U. S. C. § 2511(2)(a)(i) (1994).]

For this exemption to apply, the employer would have to be classified as a system provider or an agent of a system provider. Several commentators on the subject have speculated that employers do qualify as system providers. The term provider would likely include public email networks, such as Prodigy and Compuserve, and the term agent may or may not be defined to include employers who subscribe to or use their e-mail service. Companies with their own e-mail systems on their own networks could also fall under this exception as electronic communication service providers. Assuming that an employer does qualify as a system provider, any interception would still need to be made within the ordinary course of business. [18 U. S. C. § 2511(2)(a)(i) (1994).] Previous case law in telephone call monitoring provides some “ stare decisis” for monitoring of employee e-mail in the ordinary course of business. In both Watkins v. L. M. Berry & Co. [704 F. 2d 577 (11th Cir. 1983).] and Briggs v. American Filter Co. [630 F. 2d 414 (5th Cir. 1980).], the courts decided that if the employer had difficulty controlling

personal use of business equipment, then a personal call could be intercepted in the ordinary course of business to determine its nature, but not its contents. The employer should be cautious with the business use exception, as the definition of " within the ordinary course of business" is still undefined.

3. System Providers

Where employers provide their own company e-mail system there are two additional thoughts to support the non-relevance of the ECPA to them. The first theory is only available for employers with a system whose messages remain entirely intrastate, and is based on the ECPA's applicability being limited to interstate communications. Under this theory, an intracompany e-mail system, whose messages do not cross state lines and which is not connected to an interstate network, fails to fall under the definition of " electronic communications service," [18 U. S. C. § 2510(15) (1994).] and falls outside the protection of the ECPA. The definition of electronic communications under the law only pertains to such communication that affects interstate or foreign commerce. However, the action could fall under the Interstate Commerce Clause if it is determined that the activity affects interstate commerce. In Perez v. United States [402 U. S. 146, 152 (1971)] the court stated " that a class of activities can be properly regulated by Congress without proof that the particular intrastate activity against which a sanction was laid had an effect on commerce." Also, in Wickard v. Filburn [317 U. S. 111, 125 (1942)], the observation was made that " local activity may be reached by Congress if it exerts a " substantial economic effect on interstate commerce, irrespective of whether such effect is indirect."

Because the Interstate Commerce Clause could pre-empt this theory, the theory appears to have no basis and would be a shaky defense in a court of law.

The second theory for exclusion rests upon the ECPA's clear exemption of system providers from its prohibition against access and disclosure of stored electronic communications. [18 U. S. C. § 2701(c)(1) (1994)] The exception states " 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." Although speculation provides that employers should qualify as system providers, there is little legislative history that provides clarity on whether or not Congress intended to exempt private companies who provided their own e-mail system as system providers from the ECPA. Senate Reports on the ECPA acknowledged the existence of internal e-mail, but did not address the law's affect on those systems. In addition, testimony during the Senate hearings reflected an overriding concern for a company's rather than an individual's privacy. Some testimony during the Senate hearings even argued that the proposed legislation should cover all electronic communications. Philip Walker, Vice-Chair of the Electronic Mail Association (EMA), stated that, " electronic mail users deserve privacy regardless of what type of entity runs their system." [S. Rep. No. 99-541 (1986) Hearing on S. 1667 Before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary, 99th Congress 42 (1986)(statement of Senator Patrick Leahy (D-Vermont)).] This uncertainty of Congress has left the door open has left the door open for courts to create a narrow definition of system providers, which could only

include public, commercial providers such as America On-line, Prodigy, and Compuserve. Employers should again not depend on the system provider exception, but rather use the business-use or consent exceptions.

IV. Case Discussion

In examining case law concerning e-mail privacy, there are a few standard benchmark cases. Most of these cases come from California and it is no coincidence that this law should develop in what is considered a technological center of the United States. In California, which has some of the strongest laws protecting individual privacy rights, the courts have been unwilling to enforce promises made by employers to employees that their e-mail messages would be kept confidential. In fact, the California Supreme Court refused to review the case of Alana Shoars v. Epson America Incorporated. In that case Ms. Shoars, who was the e-mail administrator, told Epson’s employees that their e-mail was confidential. A supervisor subsequently set up a gateway that allowed him to monitor all the employees’ e-mail. When Ms. Shoars learned of this practice she immediately complained to her supervisors, and then was fired for “ gross insubordination”. The judges in Ms. Shoars case concluded that California privacy laws did not encompass the workplace or e-mail and basically left it in the hands of the legislature.

The same result was found in Flanagan v. Epson. [Sup. Ct. Cal., Jan. 4, 1991] In this case, an employee brought a class action lawsuit alleging that Epson invaded the employee’s privacy by circumventing their passwords and

reading their e-mail messages while advertising a feeling which led the employees to believe their messages were private.

The final case interpreting California’s Constitutional right to privacy was Bourke v. Nissan Motor Company. [California Superior Court, Los Angeles County (1991)] In determining whether the right to privacy has been violated, the court said you must first determine whether the individual had a personal and objectively reasonable expectation of privacy. Nissan argued that there was no reasonable expectation because the employees had signed a Computer User Registration Form, which stated, “ it is company policy that employees and contractors restrict their use of company-owned computer hardware and software to company business. Bourke and Hall countered that they had a privacy expectation because they were given passwords to access the computer system and were told to safeguard these passwords. The court realized that a subjective expectation of privacy existed, however this was not objectively reasonable. As a result, since there was no reasonable expectation of privacy, there was no violation of the right to privacy.

The federal courts seem to have taken the same position. In Smyth v. Pillsbury Corporation, [914 F. Supp. 97 (E. D. Pa. 1996).] a federal court in Pennsylvania ruled this year that Pillsbury Corporation was entitled to fire a manager who had sent e-mail critical of a supervisor, even though the company had explicitly promised it would not monitor e-mail messages. The court reasoned that an employer may not be prevented from firing an employee based upon a promise, even when reliance is demonstrated. The

court also quickly dismissed plaintiff’s claims of a tortious invasion of privacy under common and statutory law.

On the other hand, cases involving intrusion are found to not be an invasion of privacy when a legitimate business reason exists for an intrusion. In Vernars v. Young [539 F. 2d 966 (3d Cir. 1976).] an employee’s e-mail was opened and read by a fellow employee. A cause of action for invasion of privacy was found in this case. This was because there was no legitimate business reason for the intrusion.

V. Preventive Policy Measures

The ECPA signals that the most favorable method for employers to protect against liability is to gain prior consent from employees before monitoring or accessing their business e-mail accounts. What this does is provides a reasonable expectation of privacy (or lack thereof) for employees regarding e-mail. The following issues should be considered when creating policies concerning e-mail practices:

· Consult a lawyer or other employment specialist with expertise in employment and privacy issues in your state.

· Prepare a written policy.

· Include a clear description of the permissible uses of e-mail.

· Receive verification that the employees have reviewed and agree to the policies.

· Update the policies to change with technology.

· Emphasize and impermissible content for e-mails.

· Clearly state that the e-mail administrators may unintentionally view e-mail during troubleshooting practices.

· Inform employees and independent contractors of any intent to monitor e-mails.

· State the consequences of misuse of the e-mail system.

· Show flexibility by allowing limited personal use of the e-mail system but clearly define acceptable personal uses.

· Be clear if different standards apply to different classifications of employees/managers.

· Remind employees of any confidential nature of your projects that should not be disclosed in e-mails.

· Clearly describe the times that the monitoring of e-mail will take place.

· Create policies regarding the retention time of e-mails and backups of e-mail systems.

· Do not bury the policy in pages and pages of policies in a company handbook.

· Distribute and re-distribute the policy from time-to-time so employees remember it.

· Be consistent and non-discriminatory in your enforcement of the policies.

Most companies are flexible and allow for employee’s limited personal use of the e-mail system. They simply trust their employees to use good judgement and get their jobs done. Others either have written policies in place or are planning them.

Whether or not you decide to have a policy for your company, let the employees and independent contractors know if you do or do not have a policy. Clear communication is the best way to avoid disputes. It also provides for a more positive working environment.

VI. Future Privacy Legislation

Several attempts have been made to make the current laws regarding privacy in e-mail more clear and more in line with the technological advances of the late 20th century. In 1993, a bill was introduced by Senator Paul Simon (D-Ill.) to restrict employer monitoring of e-mail. The bill never came up for a vote.

The Privacy for Consumers and Workers Act has not been voted on either. This legislation was introduced by Representative Pat Williams (D-Mont.). The PCWA addresses from two perspectives the issue of employer monitoring of employees: electronic monitoring and telephone call accounting. In addressing the issue of electronic monitoring, PCWA can be analyzed in five parts: permitted monitoring, notice of monitoring, prohibited monitoring, data obtained from monitoring, and penalties.

Thought has been given to allow technological organizations, such as the Electronic Messaging Association, to govern the use of e-mail and the privacy

that users can expect. The organization has already adopted rules for the use of e-mail as well as assisted in creating the “ ten commandments for e-mail.” Those commandments (there are actually only 7) are:

· Respect confidentiality.

· Don’t flame.

· Don’t use anonymous remailers.

· Don’t look at other’s messages.

· Don’t misrepresent or lie.

· Follow EMA guidelines.

· Consider presentation of a message.

VII. Conclusion

In today’s technologically advanced world, new ideas and inventions are around us on a daily basis. A lot of these advances create opportunities for play or even danger. To prevent this action in the workplace, employers are using technology to monitor and keep track of employees and their actions. The level of surveillance being practiced by employers is unprecedented. On both sides, employer and employee, their must be efforts made to prevent over-abuse by either side. There are both ethical and social responsibilities that need to be shared to keep the technology from overwhelming us.

I hope that I have shown that the current law in this area is inadequate and needs to be reviewed. The current law in this area, the Electronic

Communications Privacy Act of 1986, does not satisfactorily address the many problems in connection with abuse of e-mail systems by employees or abuse of privacy issues by employers. The Federal Court of Appeals for the Fifth Circuit has commented that the ECPA is simply not clear and is too broad to be effective. One of the main reasons for this is that the ECPA is simply an amended version of the 1968 federal wiretap law which was originally adopted to deal with telephone eavesdropping. Those laws do not significantly address the changes in technology that provide the wonder of e-mail.

With the current legislation being ambiguous, and no new legislation yet passed, the next best solution is encouraging employers to implement a clear e-mail policy. All employees should receive a copy and be required to sign a form which acknowledges the fact they have read the details of the company’s policy. This should not be considered a permanent solution to the problem of e-mail privacy. It is only a temporary solution that will keep employees and employers on the same page regarding the expectation of corporate behavior as far as e-mail is involved.

Bibliography

VII. References

ACLU. (September, 1996). SURVEILLANCE INCORPORATED: American Workers Forfeit Privacy for a Paycheck. [On-Line]. Available: http://aclu. org/library/wrrpt96. html

AFTAB. Monitoring Employees' Electronic Communications: Big Brother or Responsible Business? [On-Line]. Available: http://aftab. com/privacy. htm

Angell, D. and Heslop, B. (1994). The Elements of E-Mail Style. Addison Wesley, Reading , MA.

Bacard, A. E-Mail Privacy FAQ. [On-Line]. Available: http://www. andrebacard. com/ema

Casser, K. (1996). Employers, Employees, E-mail and The Internet. [On-Line]. Available: http://cla. org/RuhBook/chp6. htm

Cavanaugh, M. Workplace Privacy in an Era of New Technologies. [On-Line]. Available: http://www. ema. org/html/pubs/mmv2n3/workpriv. htm

Electronic Communications Privacy Act (1986). [On-Line]. Available: http://www. tscm. com/ecpa. htm#s2511

Entwisle, S. M. E-mail and Privacy in the Workplace. [On-Line] Available: http://www. acs. ucalgary. ca/~smenwis/privacy. html

Freibrun, E. (1994). E-mail Privacy in the Workplace – To What Extent?. [On-Line]. Available: http://www. cl. ais. net/lawmsf/articl9. htm

Gan, M. (1996). Employee Rights & Email. [On-Line]. Available: http://www. newsguild. org/d6t. htm

Lee, L. Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the " Electronic Sweatshop.

Morris, F. E-Mail Communications: The Next Employment Law Nightmare. HR Advisor (July-August 1995).

Oppedahl, C. (July 3, 1995). Security, Privacy, Discovery Issues Stem From E-Mail Communications. [On-Line].

Word Count: 4313