HOW SAFE IS E-MAIL: ITS PRIVACY CONCERNS

Dr. Sudesh M. Duggal, Northern Kentucky University, duggals@nku.edu

ABSTRACT

The astronomical use of telecommunication has created concern for individuals and corporations about the privacy of e-mail. The Electronic Communications Private Act of 1986 was passed to amend Title III of the Omnibus Crime Control and Safe Streets Act of 1986, which was supposed to take care of these concerns, but it still have some gaps. This paper deals with the issues created by those gaps and how to deals with those issues.

Keywords: Communication Act of 1986, Ethical Issues, e-mail Privacy, Privacy Rights

INTRODUCTION

Information technology (IT) has enhanced business decision-making by providing unlimited access to information and has improved the efficiency and effectiveness of local and global communications. The unlimited access to information has created problems and has the potential to create future problems due to its inappropriate use. As Eining (1997) states that "The human aspect of IT, including development, marketing, management and use, raises the possibility for behavioral and social problems, including ethical issues". According to Apte (1990), "the highly concentrated storage of information in business and government organizations makes the data susceptible to theft, destruction or unethical misuse. This threatens individual privacy, corporate intelligence, and even national security".

As more firms engage in international business activities either through investment or trade, IT is increasingly being used to transfer information across national borders (Hoffman 1993). This may well worsen the behavioral and social problems from IT due to the interface between IT and people from different nations with individual national characteristics. According to Pastore (1993), "The increased globalization of information systems is another aspect of information systems that may well complicate ethical issues". Ethical issues in the development and use of IT are referred to as information ethics and deals with a series of problem areas that have special importance to those who provide, use, or are affected by IT (Mason 1986). Information ethics problems are by-products of the scope, pervasiveness and complexity of IT. The direct cause of information ethics problems, however, is typically a human misuse of IT and information.

Samoriski (1996) has voiced his concern about the new legal boundaries and its protection. According to him, "Technology is generating new legal boundaries. Laws designed to protect the conventional province of broadcast, speech, and print are proving inadequate for the domain of cyberspace, which can be defined as the domain in which electronic communication occurs and which includes computers, telecommunications, software, data, and electronic networks. Mason (1986) identified four major information ethics areas from a social orientation: privacy, accuracy, property and access. The purpose of this paper is to focus on the ethical concerns regarding privacy, in particular the electronic privacy. Electronic privacy issues are becoming more critical because of the rapidly changing, complex environments that allow users to

transmit, store, and access huge amounts of information, inexpensively and many times with little or no accountability.

ELECTRONIC COMMUNICATION

The development in communication technology have raised several privacy issues ranging from dealing with electronic databases to devices to be attached to telephones to show the phone number of the party calling. But, recently the attention is being focused on the growing network of electronic mail (e-mail) user's privacy. As Posch (1996) states that "The growth of e-mail litigation is one of the fastest areas in the United States today since the federal/state law has not kept up with the varied use of e-mail. Litigation has resulted in verdicts against employers ranging from sexual harassment (employer liable for employee correspondence it failed to monitor) to the Pentagon's leaking out intricate bombing run data over Bosnia."

Electronic Communications Privacy Act of 1986

In response to changes in telecommunications and computer technologies, the Electronic Communications Privacy Act of 1986 was passed to amend Title III of the Omnibus Crime Control and Safe streets Ace of 1968. "Essentially, from 1967-1986 the law protected only that which could be heard. The legislative history of the law notes that dramatic changes in technology no longer confined the Fourth Amendment to unwarranted searches and seizures of houses, paper, and effects. New methods and technologies for intrusion called for new laws to meet the threats to privacy imposed by those developments. The Electronic Communications Privacy Act of 1986 addressed the gaps created by advances in technology (Samoriski, 1996)." The act was intended to deal with increasing threats to privacy resulting from the growing use of sophisticated electronic monitoring devices that threatened an average citizen's reasonable expectation of privacy (Posch, 1996).

"The principal feature of the law is the incorporation of language that makes it illegal to intercept the digitized (or data) portion of a communication. The law goes on to protect computer systems in which information is stored by prohibiting unauthorized access to messages while they are in electronic storage, but exempts systems that are generally accessible to the public. In effect, the law protects private systems, but not private ones (Samoriski, 1996)." This law prohibits the intentional interception of wire and face-to-face conversation without a court order except when one of the parties to the communication has consented to such interception. "This act was worded so as to strike a fair balance between privacy rights and legitimate business practices. To violate the act, you must intercept an oral or wire communication." (Posch, 1996)

E-mail and other forms on monaural electronic data communications transmitted by a public carrier are protected under the Electronic Communications Privacy Act of 1986, which was a significant amendment to the above cited law but is integral to its definitive scheme. Prior to 1986, title 18 pertained only to wire and oral communications. It was now expanded to include "electronic " communication. The Electronic Communications Privacy Act of 1986 prohibits a third party - the police, or an individual - from gaining access to or disclosure of e-mail without proper authorization, such as consent by the user or a search warrant. Electronic Communications Privacy Act of 1986 essentially guarantees the privacy of messages sent across

public telephone line, through nations e-mail and on-line systems such as MCI Mail and CompuServe, and on cellular telephone frequencies." (Posch, 1996)

"Electronic Communications Privacy Act of 1986 excludes messages sent through a private employer's e-mail system." (Posch, 1996) "The Electronic Communications Privacy Act of 1986 prohibits the interception of e-mail messages by parties outside of a company except where there exists proper legal authorization (such as in the case of a search warrant obtained by law enforcement officials). However, the Electronic Communications Privacy Act of 1986 does not address the interception of messages by parties within a company. Thus the law is more ambiguous about whether employees are permitted to monitor and read their employees' e-mail communications." (Cappel, 1995)

"The Electronic Communications Privacy Act of 1986 does not offer such ample coverage for messages sent through a private employer's e-mail system, however. Congress defines e-mail as 'private correspondence, transmitted over public and private telephone lines. This definition encompasses internal corporate e-mail systems as well as systems available by corporate subscription or to the general public. Computer-to computer communication is also broadly defined and includes the electronic transfer of proprietary corporate information." (Posch, 1996)

Principles Governing E-mail

Smith (1994) states that, "There are certain ethical principles that should govern any and all interactive services and Users should strive for honesty, accuracy, full disclosure, and respect for the sensitivities of other users, whether this involves privacy, offensive content, commercial exploitation, anonymity, or racial or gender differences. But expectations of ethical standards, as well as expectations of privacy and security protection, differ among different categories of users."

E-mail vs. Regular Mail

"Users expect that a letter in a sealed envelope will not be opened by those not authorized to do so. So why the perception of privacy? Is it because users view e-mail in the same way they view a sealed letter? Or are they naive about computer technology? Have managers adopted explicit e-mail policy informing their employees their e-mail can be monitored? Or perhaps the social etiquette of computer-mediated communications encourages people to share their ideas and feelings, regardless of the consequences?" (Weisband, 1995) "At law, sending an e-mail message is the equivalent of sending a postcard. E-mail does not have the same constitutional free speech and privacy protections offered telephone calls and first class letters. As discussed, your employer may read business e-mail. Commercial e-mail providers don't read their customers' mail by contract or voluntary consent. There is currently no law against this. Basically, then anyone who interrupts your message in route to its final destination may read the content." (Posch, 1996)

"However, the privacy expectations of e-mail users traditionally have been most closely akin to those of regular mail users; they have operated under the general assumption that their messages are secret and confidential." (Samoriski, 1996) "It is clear that the legal system must act quickly

to adapt to this evolving means of communication. A lack of uniform actions may well result in emoting the spread of or changing the nature of what might otherwise quickly grow to the be the most efficient and utilized communications medium of the 21st Century." (Samoriski, 1996)

Users' Perceptions About E-mail

"It has been speculated that most employees underestimate the legal right of their employer to engage in e-mail monitoring activities. However, this issue has been virtually unexplored from a research respective. A study conducted by James Cappel, assessed individuals' ethical beliefs and perceptions about electronic mail privacy. This study of more than 200 e-mail users reveals that there is significant resistance to e-mail monitoring, and that may individuals have a relatively poor understanding of their e-mail privacy rights. The results also suggest that companies need to develop and communicate a policy to employees that addresses this issue." (Cappel, 1995)

"Two other reasons why subjects considered e-mail monitoring to be unethical are (1) e-mail is basically analogous to conventional mail which enjoys privacy protection (e.g. it is illegal for someone else to remove mail from your mailbox and read it); and (2) because a company set up a system of logon IDs and passwords, this presumably protects privacy and makes the reading of e-mail without permission creates and "atmosphere of distrust" in the company. A few other respondents said that it was simply "common courtesy" or "common sense" for parties not to read each others e-mail communications without permission." "Although they were in the minority, thought that e-mail monitoring is morally acceptable for one or more of the following reasons; (1) the company owns the e-mail system so it should have the right to use the system as it sees fit; (2) the e-mail system should be used only for business purposes, so the employer has a right to access it at any time, and (3) the existence of an announced e-mail monitoring policy was considered to be legitimate grounds for monitoring" (Cappel, 1995)

"In summary, individuals' acceptance of e-mail monitoring is low for several reasons, particularly because this practice is considered to be an "invasion of privacy". Even when monitoring is supported by a company policy, only a small portion of respondents thinks that is it ethical. Despite the unpopularity of e-mail monitoring, however, employees are more likely to accept monitoring when an employer has established clear worker expectations through a company policy." (Cappel, 1995)

POSSIBLE SOLUTIONS

There are possible solutions to protect e-mail messages from the invasions of privacy by other individuals or corporations, such as developing privacy policies, encryption, and new regulations such as legal means developed by congress.

Privacy Policies

"Most importantly, organizations should establish privacy policies that deal with all media of communication used by employees, rather than singling out e-mail as if is posed some unique threat to employee privacy. An e-mail policy that recognizes employee expectations of privacy

creates an atmosphere of trust among managers and employees without preventing the organization from protecting its rights and responsibilities. On the other had, such a policy requires that the organization implement more elaborate and potentially costly procedures. It asks that the company take a larger role in thinking about and responding to e-mail social and ethical issues." (Weisband, 1995)

" A clear articulation of the fact that you maintain the system solely for your business proposes. While the employee may have a personal password and the ability to delete messages as he/she see fit. Employer, as owner of the system, owns the data stored on the system including all e-mail and voice mail message in storage. "Electronic data, even when deleted can survive in varied ways and that is can be unerased. Such messages may be accessed and reviewed by state/federal government investigators upon legitimate request or even by private parties in litigation. Don't route what you wouldn't want to see in the local press." (Posch, 1996) "Tie this policy into other corporate policy (EEO and sexual harassment) and clearly state that besides no personal business being permitted, you may not send any lewd or sexual comment, defamatory comments, those that might demean another's religion, ethnic background, age, sexual orientation, national origin, disability, etc." (Posch, 1996)

Right-to-Monitor Policies: Some organizations actively monitor the messages employees send to one another, maintain that such access is necessary to properly administer the system. This urges employees to use good judgment when using the e-mail system. While right-to-monitor policies have been upheld in court, unwanted secondary effects can include increased distrust between mangers and users, in turn leading to lower morale and work productivity. User may be reluctant to use their systems for routine work communication.

Hands-off Policies: Some organizations are supportive of their employees' e-mail privacy and do not access their electronic messages. Organizations that take a hands-off approach, permitting any communications to take place electronically, might still be liable when employees use improper or discriminatory language on the company's network. E-mail policies that support privacy cannot legally guarantee it.

No-Policy: Most organizations have no formal or explicit policies regarding management's access to e-mail. If employees are unaware that e-mail messages can be intercepted and read, they have as it were a private communications medium. Having no e-mail policy is likely to create more ethical problems than having a bad e-mail policy - assuming those employees are aware of the policy. "Few employees know they can be held legally accountable for message they sent to other, as well as for messages they receive. Unlike telephone calls, e-mail messages are treated as documents that, once retrieved, can be sued as legal evidence. Ethical consequences arise when legal action is taken against individuals for communications they thought were private." (Weisband, 1995)

"User perceptions of e-mail privacy may be influenced by technology factors and the naive belief that computers are protected and secure. Users who think messages are erased when they type "delete" may be unaware the technology is capable of storing backups of their e-mail messages." "Managers who encourage open communication and participative decision making presumably do not make the same e-mail policy choices as manager who tend to be suspicious of their

employees." (Weisband, 1995) "In our race to lead the 21st century, U.S. employers must be alert to create their internal infrastructure balancing legitimate employee right to know moral issued with the employer's need to maintain a proprietary e-mail and voice mail system free of internal nuisances and in accord with its own established record retention policy. Unfortunately, most U.S. employers have failed to address these issues in a systematic way." (Posch, 1996)

Encryption

"Congress is considering legislation on definitive employer disclosure but it probably won't pass this year. The best protection available today is probably a company policy statement that lays out reasonable ground rules for inspecting employee e-mail and voice message." (Posch, 1996) "There have been questions raised as to whether the Act goes far enough in protecting privacy." (Samoriski, 1996) "Closing the gap in the Electronic Communications Privacy Act of 1986 involves the consideration of a number of developments in communication technology as well as the balancing of opposing interests." (Samoriski, 1996) "With concerns about e-mail privacy on the rise, including worries about the ease with which e-mail messages can be intercepted and altered, software engineers have devised sophisticated programs that make it nearly impossible for anyone, including the government, to peer inside e-mail messages. The process, known as encryption, involves the breading down of e-mail messages into individual codes so that only the receiver with a special key is able to decode it." (Samoriski, 1996)

"The Clinton Administration proposed to initiate a national standard for encryption in 1993." (Samoriski, 1996) Under the Clinton proposal, a standard clipper computer chip would be used to encode and decode scrambled voice and data communications with a universal key held by two independent escrow agents. When a judge authorizes a wiretap, the key holders, after identifying the particular encryption code, would transmit the key to the law enforcement agency doing the wiretap so that the message could be decoded." (Samoriski, 1996) "Opponents fought the proposal because they said the two escrow agents, the National Institute of Standards, and Technology (NIST) and a section of the Treasury Department, were not independent, but branches of the same government. The administration backed-off the proposal in July of 1994." (Samoriski, 1996) "It is apparent that encryption in and of itself does not pose any kind of final solution to the vexing problem of e-mail privacy." (Samoriski, 1996)

New Regulations

"Some other legal means must be developed to protect e-mail messages from invasions of privacy by other individuals or corporations. A possible solution consists of legislative action to extend postal regulations governing regular mail to electronic mail U.S.C. 18 1702 governing obstruction of correspondence makes it illegal for anyone to "pry into the business or secrets of another, or (who) opens, secrets, embezzles, or destroys mail before it is delivered to the person to whom it is addressed. The law covers mail while it is in a post office or authorized depository, or in the custody of any letter of mail carrier. Extending the law to the electronic domain of e-mail would encompass computer systems, disk drives, terminal and other places a message might be stored. Such an extension would resolve as many of the privacy worries e-mail users currently have." (Samoriski, 1996)

CONCLUSION

Information technology is changing at a pace that is difficult for corporations and individuals to grasp. Therefore, this rapid pace is creating ethical issues, which must be addressed. This is becoming more pressing as many corporations are using electronic mail as a means of communications. Corporations must establish policies to inform their employees that passwords do not prevent others from accessing computer accounts and that backing up electronic files is standard practice. Employers should also explain the legal implications of e-mail privacy so employees understand that messages, sent or received, can become legal documents. Since new technologies and methods of doing business bring new laws or legal exposure pending new laws. Managers need to make it clear to their employees that viewing, downloading, copying, sending, or processing information is limited to business purposes only. Policies such as these will protect the company in a variety of ways as well as informing employees of policies.

REFERENCES

Apte, U. (1990). Global outsourcing of *information* systems and processing services. *Information* Society 7 (4): 287-303.

Cappel, James J. A Study of Individuals' Ethical Beliefs and Perceptions of Electronic Mail Privacy, Journal of Business Ethics, 1995, page 819.

Eining, Martha M.; Lee, Grace M. *Information Ethics*: An Exploratory Study From An International Perspective, Journal of Information Systems, Spring97, Vol. 11 Issue 1, p1, 17p.

Hauptman, Robert**,** Library Trends, Winter2001, Vol. 49 Issue 3, p433, 8p

Hoffman, T. (1993). Bridging the *information* systems continental divide, Computerworld 27 (10): 87.

Kennedy, Ian. Journal of Medical Ethics, Jun94, Vol. 20 Issue 2, p100, 3p

Martin, E. Wainright, DeHayes, Daniel W., Hoffer, and Jeffrey A., Perkins, William C. Managing Information Technology, Second Edition, Macmillan Publishing Company, 1994 page 703.

Mason, R. O. (1986). Four ethical issues of the *information* age. MIS Quarterly 10 (1): 5-12.

Mujica, Amanda; Petry, Edward. Business & Society Review (1974), Fall99, Vol. 104 Issue 3, p279

Parker, Don B. Information Systems Security, Spring96, Vol. 5 Issue 1, p13, 6p

Pastore, R. (1993). Ethical gray matters. CIO 6 (7): 58-62.

Posch, Robert. Direct Marketing, Jan 1996, v58, page 54.

Samoriski, Jan H., Huffman, John L. and Trauth, Denise M. Electronic Mail, Privacy, and the Electronic Communications Privacy Act of 1986: Technology in Search of Law, Journal of Broadcasting & Electronic Media 40, 1996, page 61.

Smith, Robert Ellis. Ethics in an Interactive World, Business and Society Review, Fall 1994, page 48.

Strassmann, Paul A. Computerworld, 4/3/2000, Vol. 34 Issue 14, p40, 2/3p

Weisband, Suzanne P. and Reinig, Bruce A Managing User Perceptions of E-mail Privacy, Communications of the ACH. December 1995, page 40.