

December 1998

Electronic Communications vs. Privacy-Can There Be a Balance Between Progress and Individual Rights?

Jeffrey Griffin
Purdue University-South Bend

Follow this and additional works at: <http://aisel.aisnet.org/amcis1998>

Recommended Citation

Griffin, Jeffrey, "Electronic Communications vs. Privacy-Can There Be a Balance Between Progress and Individual Rights?" (1998). *AMCIS 1998 Proceedings*. 280.
<http://aisel.aisnet.org/amcis1998/280>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 1998 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Electronic Communications vs. Privacy — Can There Be a Balance Between Progress and Individual Rights?

Jeffrey A. Griffin

Computer Information Systems and Technology
Purdue University – South Bend

Abstract

The decade of the nineties has seen an explosive growth in the use of e-mail as a means of communication for both business and personal purposes. The security of information shared through e-mail, as well as privacy issues related to this communication, have been popular topics of discussion. From “The Playboy Forum” to mainstream business publications, the debate continues as to whether this communication is adequately safeguarded. This paper will discuss some of the issues related to privacy of e-mail.

E-mail Privacy Issues in the Workplace

Corporate America has embraced e-mail as the communication method of choice. It has enhanced internal, as well as external, communication for organizations worldwide. But it has also created a new set of policy problems including ownership and privacy issues.

Legislation has helped to answer some of the ownership questions. The Electronic Communications Privacy Act, which was enacted in 1986, offered corporations far-reaching ownership rights related to electronic communications including e-mail and voice mail. This Act gave corporations the right to review non-voice messages, such as e-mail, that are stored in the organization’s information systems. This right even includes unopened e-mail messages that are stored in the addressee’s electronic mailbox.

How common is corporate eavesdropping? A recent survey of businesses found that approximately 25 percent of those surveyed admitted to “eavesdropping” on their employees by reviewing computer files, e-mail or voice mail [1].

Most employees outside of the computer industry do not understand the issues related to corporate ownership of e-mail. It would be fair to assume that they have the misconception that the rights to free speech and privacy protect the e-mail they send. However, the Electronic Communications Privacy Act deems these rights as not applicable to communications sent over corporate-owned networks and systems. There are a number of court cases, which have supported the termination of employees for issues related to e-mail.

One such case, *Smyth v. Pillsbury* resulted from the firing of Michael A. Smyth, a Pillsbury employee. Smyth was terminated for “...transmitting what it (Pillsbury) deemed to be inappropriate and unprofessional comments over defendant’s e-mail system...” [2].

In another case, an employee was fired for refusing to monitor employee e-mail [3]. These cases, and others like them, have been upheld in appeals further supporting the corporation’s right to review electronic communications transmitted on corporate-owned equipment.

There is an obvious lack of understanding of the legal rights of ownership over e-mail and other types of electronic communications. And organizations, for the most part, are not adequately educating employees about the proper use of e-mail, company policies related to the ownership, review of and implications of using e-mail.

The “delete” key is another source of misunderstanding for many employees. It offers many individuals a false sense of security when it comes to electronic communications. Most large information systems have extensive back-up systems that back up information continually. Just because an individual deletes a piece of e-mail doesn’t mean that communication gone. In fact, it’s stored somewhere in the system’s archives and can be retrieved. E-mail communications are being subpoenaed frequently to settle lawsuits [4].

Privacy Issues on the Web

As home computers have become more and more affordable they have become a common fixture in millions of American homes. The explosive growth of the Internet has introduced e-mail, electronic shopping, and “browsing” to millions of people worldwide. The world is literally at our fingertips.

Most people assume that the same protections that exist for our mail exist for our e-mail. But this is not the case. Information that is transmitted on a networked e-mail system is accessible.

Imagine the outrage that would be expressed if it became customary for every piece of mail dropped in the mailbox to be reviewed by an employee of the U.S. Postal Service before being delivered to its final destination!

In many cases, each mouse click on the Web sends a signal to marketers monitoring the Internet. These tracking mechanisms, called “cookies”, tell those marketers what a person is interested in enabling companies to target potential customers for particular marketing plans [5].

Strategies for Protecting Privacy in the Electronic Age

What can be done to optimize the usefulness of today’s electronic communication technologies, while protecting the individual and business communications being transmitted?

Businesses must prepare themselves and their employees for the inevitable privacy challenges that will occur as a result of electronic communications. Corporate policies that address the writing and reviewing of e-mail should be developed within every organization with computer network technology. Although nearly 80 percent of companies in the U.S. have e-mail, less than 40 percent have company policies to address appropriate Internet usage for their employees [4].

Resources are available to assist organizations in developing these policies. Once such resource is called “Access to and Use and Disclosure of Electronic Mail on Company Computer Systems: A Tool Kit for Formulating your Company’s Policy”. The kit addresses the essential issues to be considered when formulating policy as well as describing a method for involving personnel at all levels in the development [3].

The level of privacy to be extended to employees is a corporate philosophical decision that should start at the Board level and be filtered through all levels of the organization. A balance must be struck between protecting the privacy of employees, maintaining trust and productive relationships between employees and management, and assuring the security of strategic corporate information.

As e-mail gains in popularity organizations are being formed to lead the way in developing policy related to protecting the company and the individual. The Electronic Messaging Association has been actively urging organizations to develop workplace policies and offers assistance in doing so [6].

Other helpful references for development of corporate policy include “The Internet and Business: A Lawyer’s Guide to the Emerging Legal Issues” from the Computer Law Association, as well as the Web site from North Carolina State University [4].

A second essential element in protecting privacy for the employee is to inform every employee of the company’s policy on e-mail. If it is the policy of the company to review e-mail, that must be communicated to the employees. This knowledge will enable the employee to make informed decisions when sending e-mail that could be potentially career-limiting.

But can we rely solely on the business ethics of the corporation? This author believes not.

The Pillsbury case was an important case not only because it upheld legislation which states that the e-mail was the property of the corporation. This case was troublesome because Pillsbury had a corporate policy, which stated that e-mail communications were confidential and would not be used as grounds for dismissal of an employee [7]. The court had to weigh federal legislation against a company policy, which was obviously not being followed. The decision to terminate Mr. Smyth was upheld by the U.S. District Court in Pennsylvania. Obviously company policy and the ethics being practiced by the management of the company were not adequate to avoid these electronic communication dilemmas.

Legislation such as the Electronics Communications Privacy Act can help. However, protections for the household user of e-mail need to be developed as well.

Unfortunately, through controls on technology exports the federal government has managed to limit the use of encryption. This assists law enforcement officials in the interception of potentially harmful communications. There is, however, a push to broaden the use of encryption.

An organization has been formed, Americans for Computer Privacy, whose goal is to educate the public about the advantages of encryption in such areas as protecting medical information, maintaining the security of on-line transactions and in the overall protection of people’s privacy. This group has the support of many of the major high tech companies including Intel and Microsoft [8].

In addition, Congress is beginning to respond to the growing need to protect electronic communications while maintaining the American corporation’s ability to compete in a worldwide marketplace.

The Security and Freedom through Encryption (SAFE) Act is just one bill currently before Congress. It is enjoying broad, bipartisan support and currently has 250 House cosponsors! This Act addresses the issues of broadening exports of U.S.-made encryption products while maintaining safeguards for military and weapon technologies.

Conclusion

An increasing number of industries are embracing electronic communications methods as a means of sharing information in a timely and cost-effective manner. The banking industry and health care organizations are making great strides in the development of state-of-the-art information systems. It will be imperative that the issues of privacy be resolved quickly in order to aid these relative newcomers in making advancements in electronic communications.

This author believes there is no single solution to the problem of protecting privacy of electronic communications. As the work environment continues to become more complicated and the technologies being used continue to evolve this issue of privacy of communications will continue to be difficult to address.

Through the cooperative efforts, however, of government, the computer industry, and corporations that utilize electronic communications reasonable solutions can be developed that will protect the individual, encourage continued growth of technology and maintain the U.S. position in international trade.

This paper is intended to provoke thought in an area that has recently received a great deal of attention. Meaningful action will be needed in the near future to enhance privacy protections and to insure continued progress in the expansion of the use of electronic communications.

References

- [1] Bacard, Playboy Forum, "The Computers Have Eyes: How Private is Private in the Digital Age?", *Playboy*, February 1996.
- [2] Weiner, J., "Michael A. Smyth vs. the Pillsbury Company", 914 F. Supp. 97 (E.D. Pa. 1996).
- [3] Shieh, Jackie and Rhea A-L Ballard, "E-mail Privacy", *Educom Review*, March/April 1994, Vol. 29, No. 2.
- [4] Kinney, Meghan, "Workplace Privacy: Your E-mail Isn't as Private as it Seems", *CareerBuilder*, 1998.
- [5] JunkBusters, "How Web Servers' Cookies Threaten Your Privacy", JunkBusters, 1996.
- [6] Cavanagh, Michael F. "Workplace Privacy in an Era of new Technologies", *Messaging Magazine*, <http://www.ema.org/html/pubs/mmv2n3/workpriv.html>.
- [7] McGowan, Matthew K., "Electronic Mail Privacy in the Workplace", Foster college of Business Administration, Bradley University, Peoria, IL, 1997.
- [8] Corcoran, Elizabeth, "Ads to Target Encryption Curbs", *Washington Post*, August 4, 1997.