

Managing User. Perceptions of Email Privacy



Email users, expecting privacy, risk embarrassment, lawsuits, and worse.

Suzanne P. Weisband and Bruce A. Reinig

Why do email users perceive their communications to be private when email provides virtually no safeguards against privacy violations?¹

The ethical and legal controversies regarding email are increasingly debated by computer professionals, philosophers, politicians, journalists, and legal experts. Much of the debate focuses on employee expectations of privacy in their communications and their employers' need to control and monitor the flow of information in the workplace. In most organizations, employees reasonably expect their communications to be private. They expect that a conversation in an office with the door closed is private; they expect that a letter in a sealed envelope will not be opened by those not authorized to do so. Telephone conversations are also typically perceived as private—unless callers are told the phone is being monitored. But email messages are not private. Managers can legally intercept, monitor, and read employees' email [19, 23].

So why the perception of privacy? Is it because users view email in the same way they view a sealed letter? Or are they naive about computer technology? Have managers adopted explicit email policies informing employees their email can be monitored

¹The issues of email privacy are analogous to voice mail technologies. This article focuses on email

or that it is monitored? Is it that email is mostly text-based—with few social cues and reminders of its audience—that makes it easy for people to disclose private information? Or perhaps the social etiquette of computer-mediated communications encourages people to share their ideas and feelings, regardless of the consequences?

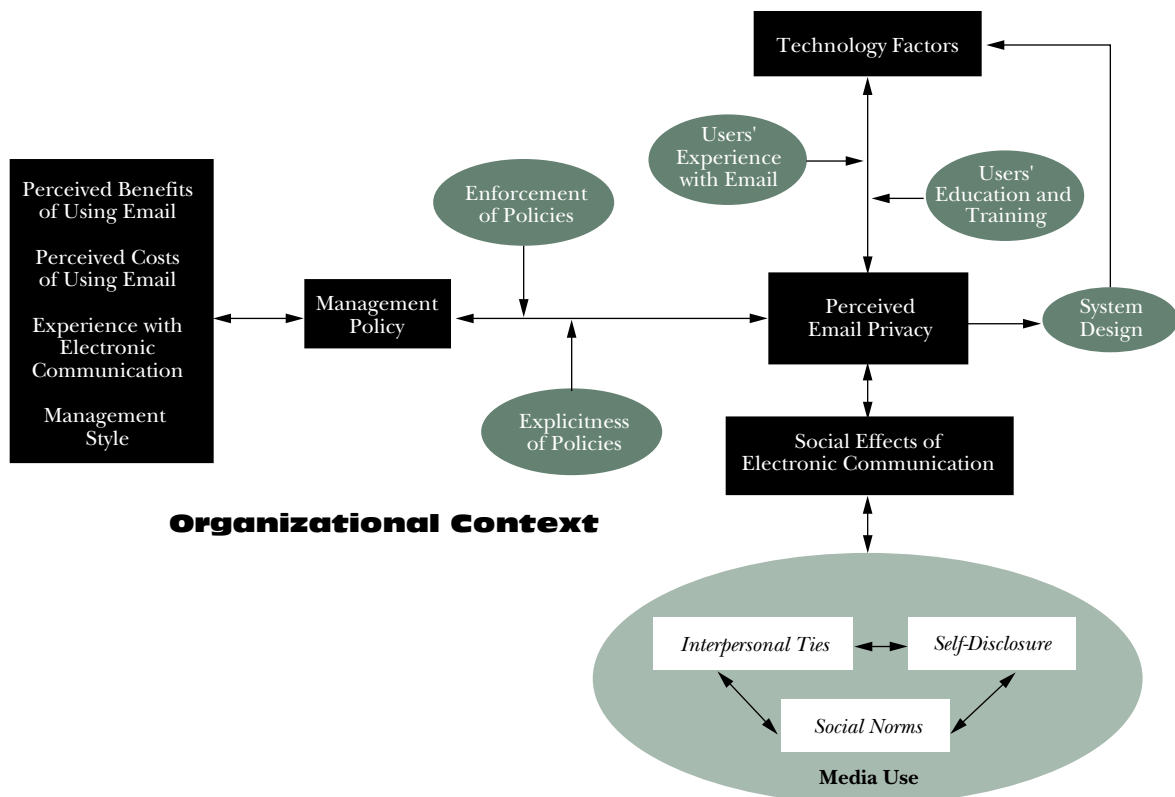
These questions illustrate the complexity of email privacy in organizations (see Figure 1). The issue of privacy violations when using email is much more complex than whether a company monitors its employees' messages. The problem is that users grossly overestimate their expectations of email privacy. For example, Rhonda Hall and Bonita Bourke were fired from their jobs at Nissan Motor Corp. in 1990 when management discovered they were receiving sexually suggestive email messages. Nissan's lawyers argued successfully that the company owned the system and had the right to read anything in it. In 1991, Los Angeles police officer Laurence Powell sent the following email message to a friend after the Rodney King beating: "I haven't beaten anybody this bad in a long time" [12]. Hall and Bourke got in trouble for messages they received; Powell got in trouble for a message he sent.

This article offers a num-

ber of theoretical explanations for why people falsely view email as private:

- User experience with and understanding of technology may support the notion of email privacy. Technology factors include hardware and software features, including interface design. The act of typing in a password may also reinforce the perception that messages are not readily accessible by anyone other than the sender. Similarly, the interface design of the email system may give the impression no one is watching.
- Management policies influence user perceptions of privacy. Organizations that fail to articulate an email policy to employees may lead users to believe they can say what they want. Organizations that explicitly stipulate email monitoring practices reduce the frequency of inappropriate messages, especially when the policies are routinely enforced. An organization's social context influences management policies. The type of work it does, the organizational goals, and social, political, cultural, and economic factors all influence the email policies adopted by management [14].
- Like any other computer-based information technology, email can have secondary social effects [20]. Email's social effects include increased access to other people and new ways of communicating with them. Because email is text-based, it involves fewer social-context cues, such as clothing, demeanor,

Figure 1. Technological, managerial, and social factors influencing perceived email privacy



and nonverbal behavior. Lacking social cues, people communicating electronically may forget the nature and size of their audience, making them feel psychologically secure in their communication. This sense of security may increase users' perception of privacy, allowing them to speak more openly, saying things through email they would not say to people face-to-face or on the telephone [21]. Open communication behavior reciprocated by others further reinforces the belief that email is private.

Ethical Consequences of Unfounded Expectations of Privacy

The apparent false perception of privacy that users have about their email has led to a number of ethical controversies, most due to what James Moor, a professor of philosophy at Dartmouth College, calls "policy and conceptual vacuums" about email in organizations [14]. Managers dealing with new choices about defining acceptable communications, whether to monitor email, and how to interpret legal guidelines, lack ways to make such choices.

Defining acceptable electronic communications may have ethical consequences. For example, managers have been known to implement email policies on the assumption that they can distinguish between business and personal messages by restricting the social dimensions of email. The Los Angeles Police Department had such a policy [12], although Powell was probably not reminded of it when he wrote of beating King. Research has shown the difficulty of separating work-related messages from nonwork-related messages since many such messages contain social and personal news [4]. The inability to differentiate acceptable from unacceptable becomes especially problematic when users communicate with people outside their own organization. Some network cultures, like universities and Internet communities, typically permit an open exchange of work and nonwork related messages, possibly conflicting with organizations that have different, more conservative social norms. The transparent boundaries in computer networks make it almost impossible to track what is an acceptable message, who receives it, and where the receivers are located.

Right-to-Monitor Policies. Some organizations actively monitor the messages employees send to one another, maintaining that such access is necessary to properly administer the system. For example, Nordstrom Department Store's policy states "email is a company resource and is provided as a business communications tool. Employees with legitimate business purposes may need to view your email messages. It is also possible that others may view your messages inadvertently since there is no guarantee of privacy for any email message." It then urges employees to use good judgment when using the email system [15].

While right-to-monitor policies have been upheld in court [23], unwanted secondary effects can include increased distrust between managers and users, in turn leading to lower morale and work productivity [9]. For example, when, in 1993, a federal judge ordered the White House and other federal agencies to preserve their email records for the National Archives, government officials took the order to mean that email was no longer safe and were reluctant to use their systems for routine work communication [8].

Hands-Off Policies. Other organizations follow a hands-off policy. According to Goode and Johnson [7], Citibank, General Motors, McDonnell Douglas, and Warner Brothers are supportive of their employees' email privacy and do not access their electronic messages. Markus [13] described one organization's use of email as being its primary medium for communications, preferring it over the telephone and face-to-face discussions. In this sense, there are few, if any, restrictions on communications content. But 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. Email policies that support privacy cannot legally guarantee it.

No Policy. Most organizations have no formal or explicit policies regarding management's access to email [17]. If employees are unaware that email messages can be intercepted and read, they behave as if it were a private communications medium. Consider the case of Robert Isaac, the mayor of Colorado Springs, who routinely examined hard copy printouts of the email messages sent and received by City Council members. The City Council had no idea its email was being monitored, and the members might have communicated differently if they knew the mayor was reading it [23]. Having no email policy is likely to create more ethical problems than having a bad email policy—assuming that employees are aware of the policy.

Legal Interpretations. Few employees know they can be held legally accountable for messages they send to others, as well as for messages they receive. Unlike telephone calls, email messages are treated as documents that, once retrieved, can be used as legal evidence. Ethical consequences arise when legal action is taken against individuals for communications they thought were private. For example, Oliver North and John Poindexter decided to use email for much of their correspondence in organizing and dispensing billions of dollars in loans to Iraq. They were undoubtedly shocked to find their email messages used as legal evidence against them. The same thing can happen to people who purportedly know better. Eugene Wang worked at Borland International, Inc.,

a software manufacturer, when he used email to allegedly send trade secrets from his current employer to his new employer [17]. Wang was caught when someone read his email, and his messages are being used as legal evidence against him.

Factors Contributing to Perceived Email Privacy

These examples of organizational email policy illustrate the apparent lack of rules or conventions regarding the use of email. Failure to develop such policies may be due to managers' inexperience or lack of knowledge of what policies ought to be implemented. An email policy must address several questions:

- Should email be treated as a private communications medium?
- Should email be used only for work-related messages?
- If email offers no reasonable expectation of privacy, how can user expectations be changed while encouraging use of the technology?

Answers require an understanding of the technological, managerial, and social factors that influence user perceptions of email privacy.

Technology. User perceptions of email privacy may be influenced by technology factors and the naive belief that computers are protected and secure. The act of logging on with a password may lead users to think their email messages cannot be accessed by anyone other than themselves. Similarly, users who think messages are erased when they type "delete" may be unaware the technology is capable of storing backups of their email messages. Several highly publicized email privacy cases were triggered when users were ignorant of system back-ups [18, 19].

As users gain experience with computers, they learn that passwords are fallible and that system administrators can access their accounts. Figure 1 shows that

interface design. System features can include software programs that filter the overload of email messages or respond to usability issues. But system designers can also address user perceptions of privacy through interface design [2]. Text-based email systems provide fewer social cues, reducing social reminders of the intended audience and possibly reinforcing the illusion the communication is private [20]. In contrast, email systems that provide a rich array of social cues are more likely to remind users their communication is not completely private. For example, social information about the communication participants can take the form of either a video icon or a message reminding the user that a particular user or group of users will read this message. Such information can remind users of the audience they are communicating with. Other interfaces can include an icon of a file drawer to remind users their email is kept in a file.

The efficacy of interface reminders alerting users of monitoring activities is not well established. Yet without them, management policies may be ignored or forgotten because people maintain their belief that computer interactions are private. Moreover, interface designers should remember their designs may have secondary effects. For example, a constant reminder that users' email is monitored may dramatically change the social structure and culture of the network. People may be more careful about the groups (bulletin boards and distribution lists) they join and the people with whom they communicate.

Management Policies

Given the Internet's increasing media attention and the need for businesses to get connected [22], most managers probably bought email systems without thinking carefully about policies for using them. Such decisions illustrate the policy vacuum surrounding email and suggest that managers' adoption of email policies is influenced by a number of factors. Figure 1 lists four factors associated with these policies. One

Users learn that passwords are fallible and that **system administrators can access their accounts.**

users learn through experience and education to be aware of the privacy risks associated with email and modify their behavior accordingly. Others may turn to encrypted software to ensure their privacy. Through encryption, users can encode messages so that only the intended recipient can read them. Effective encryption might, in theory, protect individuals. But unless encryption is implemented automatically and routinely, users might ignore it, thinking it unnecessary [10].

Technology factors associated with perceived privacy risks may also require changes in system features and

important consideration is how managers view email benefits and costs. Managers focusing only on the productivity benefits of email may fail to anticipate the larger social consequences. Experience with previous email systems may also influence management's decisions about email policy. For example, managers with positive experiences make different choices from managers who fear or question email use. In addition, management style is likely to influence local managers' policy decisions. Managers who encourage open communication and participative decision making presumably do

not make the same email policy choices as managers who tend to be suspicious of their employees.

Perceived Benefits. Table 1 lists some of the benefits and costs associated with email software for private communications. Benefits include cost savings, efficiency, documentation, access to resources, and monitoring. Email is viewed as cost-effective because it is much cheaper to send electronic messages over long distances than it is to make telephone calls or send faxes. It is also perceived to be an efficient form of communication because it avoids telephone tag, is faster than the U.S. Postal Service, and users can send messages to hundreds of people as easily as they can to one person. With email, managers can document and store their correspondence with others, keep track of their work flow, and evaluate employee performance. Managers and their employees also gain access to information resources in the form of archives and databases, as well as to each other. We cannot rule out the possibility that management's decision to buy email systems is due in part to its ability to monitor employee communications to identify inappropriate behavior and breaches of company policy.

Perceived Costs. How people use email in organizations does not always conform to management's expectations of how the organization thinks it should be used. At times, the perceived benefits of increased productivity and efficiency are affected by such unforeseen social costs as unwanted or inappropriate forms of communication, as well as by too much communication. Management then implements email policies to reduce these potential costs. For example, to reduce offensive or frivolous email, management may explicitly monitor employees' email to catch those who use the medium inappropriately.

When email messages proliferate faster than people can read them, users become overwhelmed by the files in their electronic mailboxes, and managers worry

only receive messages. Editors, on the other hand, could still use email to send and receive messages [21].

Experience. Like their employees, managers have varying experience with email. Those without computer communications experience may be unaware of the need to have an explicit email policy, or they may implement policies without thinking of the larger social context in which email is used. Doing so, they overlook the need to inform their employees of company expectations regarding employee email, setting up a potential conflict between user expectations of privacy and management's productivity goals. Managers' email policies may also be influenced by their email experience. The decision to shut down Computer Associates' email system was mostly the result of Wang's negative experiences with email [24]. Positive experiences with email may be reflected in policies that support its use for all communication activities [13].

Management Style. Email policies and communication privacy considerations may also depend on management style. Managers who tend to trust their employees would be less likely to monitor messages than would managers who tend to be suspicious of their employees. Some managers believe it necessary to control employees' work performance, micromanaging every job responsibility; other managers prefer to delegate responsibility, granting employees freedom to manage themselves. This suggests that individual management styles influence email policies in different ways.

After email policies are adopted, user perception of privacy is influenced by their enforcement, as well as by their explicitness (see Figure 1). To avoid catching email users off-guard, policy enforcement is especially important if users think their communication is private. With few social reminders, email provides an opportunity to write things that may later be deemed regrettable. Enforcement and explicitness of a company's email policy is critical to ensuring that employ-

Why do people disclose personal and sensitive information on a computer? Mainly, it is psychologically easier to self-disclose when no one is looking.

employees are not getting their real work done. For example, Charles Wang, Chairman of the Board and CEO of Computer Associates International, shuts down his company's email system five hours a day to discourage frivolous emailers [24]. Management policy to control inefficient email includes restricting the kinds of messages that can be sent. In an extreme case, the management of the New York newspaper *Newsday* wanted to prevent reporters from spending too much time on the system and modified its software so reporters could

ees are not only aware of the policy, but follow it. Failure to do so reinforces the perception that no one is watching.

As Figure 1 shows, management policies and decisions are implemented in an organizational context. That is, the social norms and values and the organizational culture influence adoption of email policies. Some organizations, such as universities and research centers, encourage freedom of expression and value diversity of opinion. Other

organizations are more cautious about the kinds of communication they permit. Such communication policies as restricting personal phone calls or following proper communication channels can be found in many government agencies, as well as in other bureaucratic organizations. Companies concerned about protecting trade secrets legally bind their employees from revealing secrets they learn at work. As employees become socialized to these organizational norms and values, the organizational context provides an important determinant of how people perceive communications privacy in general and email privacy in particular.

Social Effects

The organizational and social contexts of all communications influence not only user perceptions of privacy, but also how users use the various media [5]. By increasing access to other people and by creating new ways of interacting with them, the social effects of email directly affect the way people make sense of their personal experience [5]. Assimilation of other people's behaviors and attitudes gives meaning to the events email users experience on the network. Since the interpretation of email messages is subjective and socially constructed, communication on the network results in different perceptions of email privacy for both individuals and organizations.

How do email's social effects influence user perceptions of privacy? Research suggests new computer communication technologies can change the social constraints on communications by reducing the social-context cues—information about social hierarchy, social differences, relationships, and the personal meaning and implications of interaction [20]. Because email users typically do not see the person or persons with whom they interact, email reduces self awareness and makes people believe they are more anonymous. The result can be more open discussions in the exchange of email messages. Figure 1 shows how these social effects influence media use. Email creates the perception of privacy through social norms, mutual self-disclosure, and development of interpersonal ties.

Social Norms. Media use is influenced by social norms. Social cues regarding appropriate media use may be embedded in the norms of a particular group or within an entire organization. For example, in a study conducted by Markus [13], social norms directly influenced the organization's use of email, and also affected its use of other communication media. With-

out the reminders of an audience, users become less constrained by the norms of conventional behavior and develop social norms appropriate for the particular technology. The phenomenon of "flaming" in electronic discussions suggests people lose their fear of social sanctions and criticism due to limited reminders of conventional human interaction [21]. In her study

Table 1. Perceived benefits and costs of using email

Benefits	
+ Cost Effective	(cheaper than telephone/fax/mail)
+ Efficiency	<ul style="list-style-type: none"> • Reduced telephone tag (speed) • Group distribution lists
+ Documentation	(organizational memory) <ul style="list-style-type: none"> • Storage • Back-up
+ Access to Resources	<ul style="list-style-type: none"> • Information (databases and archives) • People (knowledge and expertise)
+ Monitoring	<ul style="list-style-type: none"> • Improved scrutiny of employee communications • Gauge productivity and workflow • Give employees managerial feedback
Costs	
- Offensive communication	(flaming) <ul style="list-style-type: none"> • Open communication leads to inappropriate behavior
- Frivolous Use	(playing and socializing) <ul style="list-style-type: none"> • Email is fun and self-absorbing • Real work is less important
- Information Overload	<ul style="list-style-type: none"> • Email becomes dominant form of communication • Organizational norms encourage employees to read all messages • Email is difficult to organize and manage

of "Drugcorp," Shoshanna Zuboff, a professor at the Harvard Business School, quoted a respondent as saying, "When I discuss something on DIALOG, in the back of my mind I know somebody else is going to hear it, but it isn't as obvious as if we were all in one room. It's like I know the tape recorder is running, but I kind of block it out" [25]. Thus, with few reminders of who they are communicating with, people believe they are free to express themselves and to self-disclose, perceiving they have more privacy than they really have.

Self-Disclosure. Why do people disclose personal and sensitive information on a computer? Mainly, it is psychologically easier to self-disclose when no one is looking [11]. Psychology experiments examining the effects of self awareness on self-disclosure have found that intimate self-disclosure is unpleasant for subjects disclosing in the presence of a large mirror, as compared to subjects who disclose without a mirror [1]. This research concludes that reduced self awareness—by taking away the mirror and the audience—redirects people's attention from their weaknesses and faults, making them feel safe saying what is on their minds.

Moreover, there are social benefits from self-disclosure derived from the reactions of other people. Many types of social support can be provided through self-

disclosure in a relationship, including esteem support, informational support, instrumental support, and motivational support [3]. The growing number of bulletin board systems and online computer conferences offering social support attests to the ease and low cost of discovering people with common interests.

Interpersonal Ties. Self-disclosure, especially of a personal nature, figures prominently in development of interpersonal ties [6]. Self-disclosure occurs as part of ongoing social interactions between participants who determine jointly what, when, where, and how they communicate with one another, including whether to self-disclose. With reduced social-context cues, and the relatively low cost of meeting people with similar interests, email can increase the number of potential ties available [16]. As interpersonal ties develop, the opportunity for mutual self-disclosure also increases. And as more people mutually self-disclose, the more knowledge they have of each other and the greater their investment in each other's well-being and efficacy [6].

Although some online communities, including bulletin board systems and company distribution lists, have developed strong social norms of behavior, behavior in electronic situations remains quite varied. Due to the uncertainty about what is appropriate communication etiquette, people learn the social norms attached to the technology through observation and imitation. When employees observe the exchange of what seems to be rather private disclosures of others or the open expression permitted on the network, they may believe that such personal communication is the norm, not the exception.

Consider the increasing number of businesses entering the Internet [22] through which employees are subject to diverse communication behaviors, not all of them tasteful or acceptable. Ethical controversies on the Internet include the definition of appropriate content, freedom of electronic speech, and whether and how communications should be policed or censored. We are still working to define the social norms of computer-mediated communications, and organizations without rules and norms for using email have difficulty guiding user behavior. Perhaps as people become more familiar with the technology, social norms will stabilize and management policies will be more effective.

Conclusions

Perceptions of email privacy result from three factors:

- Technology and users' knowledge and experience;
- Management policies in an organizational context; and
- The psychological effects of email that encourage self-disclosure, development of interpersonal ties, and new norms of social behavior (see Figure 1).

As long as email has few social cues and seems ephemeral, users may communicate more openly

and with less discretion than they would otherwise. The implication is that employers are obliged to inform and educate users about their specific email policies, as well as about technology factors and computer security issues. Employees must learn that passwords do not prevent others from accessing computer accounts and that backing up electronic files is standard practice. Employees should also understand the legal implications of email privacy so they are not surprised when messages they send or receive are used to document some undesirable behavior. Interface design issues could address this by reminding users that deleted messages are not sent to a trash can but to a filing cabinet.

More importantly, "organizations should establish privacy policies that deal with all media of communication used by employees, rather than singling out email as if it posed some unique threat to employee privacy" [9]. In an article prepared for the Electronic Messaging Association in 1994, Johnson and Podesta [9] spelled out what employers need to consider when formulating their email policies. Such policies require organizations to think about and respond to several questions, including:

- Who has a stake in establishing email policy?
- What baseline legal rights and duties constrain any email policy?
- What criteria should be used to evaluate a proposed policy?
- Has the policy been disclosed in advance?

An email 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 hand, such a policy requires that the organization implement more elaborate and potentially costly procedures [9]. It asks that the company take a larger role in thinking about and responding to email's social and ethical issues. ■

References

1. Archer, R., Hormuth, S., and Berg, J. Avoidance of self-disclosure: An experiment under conditions of self awareness. *Personality and Soc. Psych. Bull.*, 8 (1982), 122-128.
2. Bellotti, V. and Sellen, A. Design for privacy in ubiquitous computing environments. In *Proceedings of ECSCW '93 Conference* (Sept. 13-17, Milan, Italy). Kluwer Academic Publishers, Boston, 1993, pp. 77-92.
3. Derlega, V., Metts, S., Petronio, S., and Margulis, S. *Self-Disclosure*. Sage, Newbury Park, Calif., 1993.
4. Finholt, T. and Sproull, L. Electronic groups at work. *Org. Sci.*, 1 (1990), 41-64.
5. Fulk, J., Schmitz, J., and Steinfield, C. A *Social Influence Model of Technology Use*. In Fulk, J. and Steinfield, C. (Eds.), *Organizations and Communication Technology*, pp. 117-142. Sage, Newbury Park, Calif., 1990.
6. Gabarro, J. *The Development of Working Relationships*. In Galegher, J., Kraut, R., and Egido, C. (Eds.), *Intellectual Teamwork: Social and Technical Foundations of Creative Work*. Erlbaum, Hillsdale, N.J., 1990.
7. Goode, J. and Johnson, M. Putting out the flames: The eti-

- quette and law of email. *Online* (November 1991), 61-65.
8. Johnson, D. *The law of Computer Communications and Networked Communities*. Tutorial presented at the CSCW '94 Conference (Oct. 22-26, Chapel Hill, N.C.).
 9. Johnson, D. and Podesta, J. *Privacy Toolkit: Access to and Use and Disclosure of Electronic Mail on Computer Systems*. Prepared for the Electronic Messaging Association, September, 1994.
 10. Kiesler, S., Sieff, E., and Geary, C. The illusion of privacy in human-computer interaction. Working Paper, Carnegie Mellon University, Pittsburgh, Penn., November 1992.
 11. Kiesler, S. and Weisband, S. Self-disclosure in computer surveys, interviews, and psychological tests: A meta-analysis (in review), September 1995.
 12. Kuebelbeck, A. Getting the message. *Los Angeles Times* (Sept. 4, 1991), D1.
 13. Markus, M. Finding a happy medium: Explaining the negative effects of electronic communication on social life at work. *ACM Transactions on Information Systems*, 12 (April 1994), 119-149.
 14. Moor, J. What is computer ethics? *Metaphilosophy*, 16 (1985), 266-275.
 15. Nelson-Rowe, L. *Open Systems Today*, (Oct. 12, 1992), p. 22.
 16. Pickering, J. and King, J. Hardwiring weak ties: Individual and institutional issues in computer mediated communication. In *Proceedings of CSCW '92 Conference* (Oct. 31-Nov. 4, Toronto, Canada). ACM Press, 1992, pp. 356-361.
 17. Piller, C. Bosses with x-ray eyes. *MacWorld*, 10 (July 1993), 118-130.
 18. Rifkin, G. Do employees have a right to electronic privacy? *New York Times*, 1991.
 19. Shannon, J. and Rosenthal, D. Electronic mail and privacy: Can the conflicts be resolved? *Business Forum*, 18 (Winter/Spring 1993), 31-34.
 20. Sproull, L. and Kiesler, S. Reducing social context cues: Electronic mail in organizational communication. *Manag. Sci.*, 32 (1986), 1492-1512.
 21. Sproull, L. and Kiesler, S. *Connections: New Ways of Working in the Networked Organization*. The MIT Press, Cambridge, Mass., 1991.
 22. Verity, J. The internet: How it will change the way you do business. *BusinessWeek* (November 14, 1994), 80-88.
 23. Witt, L. Terminally nosy: Are employers free to access our electronic mail? *Dickinson Law Rev.*, 545 (Spring 1992).
 24. Zachary, G. It's a mail thing: Electronic messaging gets a rating—ex. *Wall Street Journal* (June 22, 1994), A1.
 25. Zuboff, S. *In the Age of the Smart Machine*. Basic Books, New York, 1988.

About the Authors:

SUZANNE P. WEISBAND is an assistant professor of MIS at the University of Arizona. Her current research interests include how personal status affects electronic groups, information sharing, performance in remote work groups, and the effects of self-disclosure on computer assessments. **Author's Present Address:** Department of Management Information Systems, College of Business and Public Administration, University of Arizona, Tucson, AZ 85721; email: sweisband@bpa.arizona.edu

BRUCE A. REINIG is a Ph.D. candidate in the Department of MIS at the University of Arizona. His current research interests include the management of and social policies needed for information technology, groupware for improved learning, and diffusion of information technology. **Author's Present Address:** Department of MIS, College of Business and Public Administration, University of Arizona, Tucson, AZ 85721; email: breinig@bpa.arizona.edu

Permission to make digital/hard copy of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication and its date appear, and notice is given that copying is by permission of ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.