'E' for exposed? E-mail and privacy issues

Pat Gannon-Leary
E-mail: p.m.gannon-leary@hud.ac.uk

In March 1996, American Libraries *featured a piece about a librarian at the University of California/Irvine whose supervisor intercepted her e-mail while she was absent on medical leave. As a result of this, UC's Office for Academic Computing began a review of e-mail privacy on the nine-campus system. This article and UC's reaction prompted my research into this topic.*

Declaration of intent

A number of American companies now have written policies declaring sovereign power with regard to electronic communications. Employees are made aware of such policies at orientation, where it is explained to them what will be monitored, by whom and why; they will be advised on inappropriate content of messages — for example harassment or hate mail — before being asked to sign an acknowledgement that company policy has spelled out the corporate role. A log-on initial screen may reinforce the policy by reminding them that the company monitors messages. Some companies give their employees a certain amount of disk space for personal use, with the undertaking that no one will use that space improperly. The introduction of such policies has resulted from litigation involving some US companies, and employers hope these measures lessen the threat of privacy issue lawsuits.

It is important that companies be up-front about their policy and intentions. It would also be helpful if employees were aware of just how far down the road technology has gone and what its capabilities are. Corporate computer systems may save and store data automatically for a number of years partly to ensure against data loss if a system crashes. Sophisticated retrieval programs mean that even deleted files may be reconstructed. It's also possible to divert incoming e-mail messages to another account. So who would want to review or divert an employee's mail randomly? Research indicates that Information Systems and Human Resources are the most likely reviewers, rather than Security/Legal departments or supervisors (Kanner 1996).

One might assume, because the introduction of such policies was the result of legal issues, that Security or Legal departments were most likely to be interested in the content of e-mail messages, especially where corporations are required by law to provide lawyers with a list of available electronic data. While e-mail access may constitute an invasion of an employee's privacy, it could also be perceived as reducing company liability resultant from employee malfeasance in the case of communications which might be deemed discriminatory or libellous and, as such, might be requested by attorneys during discovery. The legitimacy of the legal right to read e-mail sent over a company network is surely dependent on certain situational and organisational factors. Defence organisations are highly conscious of e-mail issues and monitoring may be justified as a security measure to ascertain that employees are acting in the organisation's best interests, safeguarding 'company' secrets and assets.

So why would Information Systems be looking at employees' e-mail? Network administrators have to monitor e-mail storage to ensure it is not having an adverse effect on network performance and to control communication costs, but would this necessitate their reading the content of what is, in effect, a letter? Computer files could be (mis)handled in a variety of ways, some of which may fail to differentiate between personal messages and confidential material.

Balancing act

Companies need to balance the rights of employees against their own needs with regard to system security and deployment of company resources. If an e-mail policy states that all such messages are company policy, this may inhibit employees to an extent that is detrimental to the company and its mission, destroying the potential of the communication medium. Management may feel that, if the company owns the computer, then it is entitled to review files contained on this equipment which was purchased to enable employees to carry out their designated duties. What if the employee uses company equip-

ment, possibly in company time, for the transmission of personal messages? In such instances, can he or she expect the same right of privacy granted to phone conversations and snailmail letters? Long distance phone calls may be monitored by an employer to check that these are not being made for personal purposes, so might e-mail monitoring be deployed similarly?

Why are Human Resource departments reviewing e-mail messages? Surveillance may be used in appraisal — checking on employees' abilities by listening in to their phone calls is not unknown (although in some states it is illegal to eavesdrop on phone calls even when made on a company-owned phone). Might e-mail surveillance be used as an evaluative tool also? While the 1984 ('Big Brother is watching you') aspect may be alarming, such a practice might improve a company's productivity, make employees more accountable and raise their performance because they never know when they're under observation. This type of activity might be seen as the company's right to control, monitor and evaluate its personnel.

What happened to freedom of speech and the right to privacy protected in other arenas? The arguments that hate mail and pornography are transmittable via e-mail don't hold water with civil liberties advocates. Management monitoring of employees' e-mail is ethically questionable. Naturally, employees may see all these issues in a different light from their employers — as invasion of privacy, as having the potential for misuse (just what might the company do with information found?) and infringement of constitutional rights. They may fear that the company could use surveillance for performance monitoring and the basis for dismissal. If an intercepted e-mail message were critical of management or the organisation, might this be grounds for termination? What about the status of forwarded messages with controversial content? As a matter of courtesy recipients should probably ask permission from senders before forwarding their messages to A.N. Other but this is not always considered; nor is the question of who owns the copyright of that message, sender or recipient? Or — if it is on the company network, created in company time — the 'boss'?

I'm no lawyer so I have not raised the legal arguments. This is just a brief expression of concerns raised by my own use of e-mail. It boils down to everyone's wanting to mind their own business. Employers wants to safeguard their company: we employees are anxious to protect our privacy and constitutional rights.

The library situation

As library employees, are we able to do so? I contacted, via listservs, libraries in the USA and the UK asking if they were aware of any monitoring of their e-mail. The response to the query from the UK academic library sector was 'Good grief! No!', but some American university libraries provided examples of login messages, for example:

> *Welcome to the computing resources located at the University of X. Use of these resources is governed by University and Regental policies, as well as State and Federal statutes. Protecting an individual's right to privacy is of paramount importance, but please note that accounts may be monitored by the System Administrator if there is evidence of misuse.*

Each account holder at the above university signs an agreement indicating that he or she will abide by system policies.

Another American university librarian reports that their e-mail isn't monitored. The policy there is that personal use is 'incidental' to doing one's job. The only problems come from people having so much e-mail that it's clogging up the system.

Staff at one American Community College sign a statement when they receive their e-mail account which notifies them that their e-mail activity *may* be monitored. My respondent knows the Computer Centre checks Internet use regularly but doesn't know how often it checks e-mail.

The Circulation Manager of another American university library has been involved in a group that is drafting guidelines for employee use of e-mail. In the US there are still some legal questions about what constitutes 'monitoring' versus 'interception' of employee mail. What the group decided, however, was that as a public institution any of its records were considered public, so it states as much to its employees. It has a page a couple of paragraphs long which employees will have to sign, stating that they understand the e-mail use guidelines and agree to abide by them.

An Australian university librarian tells me that they have not been advised of any monitoring of their e-mail and have only been asked not to put any other addresses or interests outside of work in the signature. By outside interests, they mean that if you happen to be an office bearer in some other organisation or interest group then you should not list a contact address in the work e-mail address.

Inspection of Web sites of academic institutions revealed that most of these, both sides of the Atlantic, have an acceptable use or netiquette policy of some sort, usually issued by Computing Services. In the USA many high schools also produced such a policy online, along with copies of the form which students and their parents had to sign prior to their being issued with a password to access the system. Some even included a Network Access Orientation assignment to be completed by students to confirm their awareness of requisite procedures. With high school students the primary aim is, presumably, that parents are informed that the school cannot guaran-

tee their children will not access sites with pornographic or other unsuitable content, and the school is covering itself against prosecution by parents.

Such policies as those above do not refer to e-mail alone but most contain advice about e-mail. For example, they recommend consideration of e-mail as equivalent to a postcard rather than a sealed letter; and advise that the writer not convey any message electronically that he or she would not mind appearing in a newspaper, and avoid sending sensitive material via electronic means unless employing an encryption program. They stress that e-mail is neither completely private nor secure and that, due to occasional security breaches at sites across the Internet, it may be seen by a system cracker or intruder. Despite best efforts to prevent it, there is the possibility that a determined person could gain unauthorised access to stored data and violate e-mail privacy.

Spelling it out

A typical e-mail section of an Acceptable Use Policy, or Ethics Policy, or Guidelines to the Use of Electronic Mail document includes a warning along the following lines:

> *While the University of X supports the privacy of electronic mail, users must assume that e-mail messages are not secure and therefore cannot be guaranteed to be private. System Operators do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities and may result in loss of user privileges.*

They also usually advise against forwarding confidential e-mail received to another person without obtaining the permission of the originator of the message.

Generally, institutions spell out what e-mail is and what it should not be used for (for example mass electronic mailings):

> *Electronic mail is a fast, convenient form of communication. It is easy to send electronic mail to multiple recipients, and you can even send a message to many recipients simply by specifying a single list name. Sending mass electronic mailings consumes large amounts of disk space. There are alternatives far more efficient. Any distribution to more than 25 recipients must be cleared in advance with the Computing Centre. These guidelines are not based on etiquette alone: the mail system simply does not have the capacity to process a very large number of e-mail messages at once. When a user sends out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a negative impact on the quality of service provided for all users.*

> *The proliferation of electronic chain letters is especially abusive of the mail system and the network. Chain letters are an illegal use of e-mail and can cause excessive loading of mail facilities, they waste valuable computing resources, and may be considered harassing. Creating or forwarding chain letters may subject you to Institute disciplinary proceedings.*

The above indicates that institutional harassment policies extend to the networked world, and that the sending of e-mail or other electronic messages which unreasonably interfere with anyone's education or work at the university is in violation of the intended use of the system and may constitute harassment. You may feel you have the right of freedom of expression, but others have the right to be free from harassment.

Inclusion of e-mail harassment in wider harassment policies stresses the fact that all institutions have rules for acceptable behaviour, and extend these rules to encompass procedures governing the use of information networks:

> *Institutional code of conduct applies to network activities as well. Therefore, the Acceptable Use Policy is an extension of the institution's behaviour code. It is a general policy that all computers are to be used in a responsible, efficient, ethical and legal manner. Illegal activities shall be defined as those which violate local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the network, and/or purpose and goal. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication systems.*

Universities also stress that they are striving to provide fair and distributed access to computing and network facilities for a large number of users. Proper use follows the same standards of common sense, courtesy and restraint in the consumption of shared resources that govern use of other public facilities. Improper use violates those standards by preventing others from accessing shared facilities.

Bill of rights

We might feel more confident and content about using e-mail if our employers produced a document like a charter which spelled out its expectations of us with regard to use of e-mail, and guaranteed certain rights to us: for example acknowledging that we, as users, have the right to keep certain data reasonably confidential, such as electronic mail correspondence, and that we have the right to be informed of

what the limits of confidentiality are in the system. Any such charters or policies need to be more widely disseminated, or at least drawn to the inductee/employee's attention. All members of the organisation need to assume responsibility for providing reasonable publicity for the Acceptable Use Policy at their sites, and for communicating both this policy and the fact that the ultimate responsibility for traffic which does not conform to this policy is with the individual end-user who originates that traffic.

British universities usually have an Acceptable Use Policy formulated by Computing Services which is applicable not only to e-mail but all IT facilities provided by any schools, departments or sections of the university. These are often based on the JANET Acceptable Use Policy, or may require their members to abide by the JANET Policy

Most such policies stipulate that the primary reason for the provision of university computing resources is to facilitate a person's work as an employee or student of the university, specifically for educational, training, administrative or research purposes. Occasional use of local campus networks for personal electronic mail is not generally considered improper as long as these: are in keeping with the framework defined in the Acceptable Use policy document; do not interfere with one's duties, studies or the work of others; and do not in any way bring the university into disrepute. If abuse occurs, privileges may be withdrawn as part of a disciplinary procedure. Without specific authorisation, all activities using institutional facilities for personal profit or for the direct financial benefit of any outside organisation are prohibited. However, this does not apply to normal communications and exchange of electronic data, consistent with the university's education and research roles, that may have an incidental financial or other benefit for an external organisation. For example, it is appropriate to discuss products or services with companies doing business with the university, or to contribute to Usenet bulletin boards discussing issues relating to commercial products.

It is helpful if the employer outlines limitations on privacy, for example:

> *The institution has the right to monitor what you do on the network to make sure that the network continues to function properly for all of its users. Your files may be accessible by persons with system privileges, so do not maintain anything private in your disk storage area.*

> *During an investigation the Computing Centre reserves the right to copy and examine any files or information resident on Computing Centre systems allegedly related to the improper use, including the contents of electronic mailboxes. Investigations that discover improper use may cause the Computing Centre to disclose information found during the investigation to other University authorities.*

> *You should realise that unauthorised access to information is possible through malicious mischief, particularly if you are careless about protection of your passwords and the use of system security features. You should be careful about storing or processing sensitive information. The Computing Centre cannot guarantee the protection of information from unauthorised access. To impose more stringent security measures on these computer systems would impede your access to them and would prevent the Computing Centre from fulfilling its primary function in support of research and education.*

> *Institutional policy is to ensure the greatest degree of confidentiality in treating user data on its systems and networks consistent with available technology and the need for system backups, troubleshooting, etc. The situation will vary somewhat depending on what system or network is being used. Users should be aware that data storage and communications are not perfectly secure; there are software and physical limitations that can compromise security. The institution tries to minimise such exposures, but the risks exist, e.g. a bug in a utility program might allow one user to read another's files, or a user might tap a data network wire to view data that is flowing to another user's machine. Data files residing on disk are periodically backed up to magnetic tape, and some of these backups are retained for long periods of time. All user files may be backed up this way*

> *Certain utility programs allow users to view other users' activity on a computer system or network.*

> *Certain system activities are routinely logged, and the logs may be readable by other users. The intention of logging is to collect statistics and diagnose system problems, e.g. logs of mail messages sent or received may be kept. In cases of suspected violations of institutional policies, especially unauthorised access to systems, the director of the facility concerned may authorise detailed session logging. In addition, s/he may authorise limited searching of userfiles to gather evidence on a suspected violation.*

It is reassuring if the institution undertakes, despite such limitations, to make all reasonable efforts to maintain confidentiality of user data, for example:

> *Employees are forbidden to 'browse' user files without specific purpose and authorisation. If, by mistake or other cause, an employee reads protected user information, they will not divulge this information except as authorised by the director of the facility concerned or by appropriate legal authorities. The institution reserves the right to review any material on user-accounts and to*

monitor fileserver space in order to make determinations on whether specific uses of the network are inappropriate. In reviewing and monitoring user-accounts and fileserver space , the institution shall respect the privacy of user-accounts.

Some American institutions have drawn attention to the guidelines for access to information established in the Library Bill of Rights of 1980 and liken the Internet to a vast digital library. In defining the Internet's resources as an extension of the Library, an institution can subscribe to the Library Bill of Rights' avowal that 'A person's right to use a library should not be denied or abridged because of origin, age, background or views.' In return, as in a charter suggested above, every account holder is expected to respect and protect the rights of all others in the community and on the Internet; and to act in a responsible, ethical and legal manner in accordance with any policies, whether they be Acceptable Use Policies, Ethics Policies, Codes of Conduct, the missions and purposes of networks used on the Internet, and laws both local and national.

Reference

KANNER, B. (1996) With e-mail replacing snail mail, privacy's a dilemma, *Jackson Clarion-Ledger*.

Further reading

BEESON, A. (1996) Top ten threats to civil liberties in cyberspace, *Human Rights*, 23(2), 10-13.

BLANTON, T. (1995) New rules for the e-mail generation: lessons the White House learned the hard way, *Washington Post*, 26 November, C2.

DANCA, R.A. (1993) Privacy Act would force firms to inform their employees about e-mail monitoring, *PC Week*, 18 June, 203-204.

FRYER, B. and R. FURGER (1993) Who's reading your screen? *PC World*, August, 166.

'Librarian battles over e-mail privacy' (1996) *American Libraries*, March.

MARX, G. (1992) Let's eavesdrop on managers, *Computerworld*, 20 April, 29.

MILLER, M. (1995) Should e-mail be private? *Los Angeles Times*, 12 November, A3.

MOHAN, S. (1994) Users still wrestle with e-mail privacy: lack of clearly defined policies leave many wary, *Computerworld*, **28**(50), 12 December, 24.

MORSE, A. (1995) University e-mail a test of Internet free speech, *Los Angeles Times*, 10 December, M2.

NARISETTI, R. (1996) E-mail snooping is OK in the eyes of the law, *Wall Street Journal*, 19 March, A1.

PEYSER, M. and S. RHODES (1995) When e-mail is oops-mail, *Newsweek*, **126**(16), 16 October, 82.

SALAMONE, S. (1991) Attorney discusses how to avoid e-mail privacy woes, *Network World*, 25 March, 21.

SAMUELS, P.D. (1996) Who's reading your e-mail? maybe your boss, *New York Times*, 12 May, F11.

SKUPSKY, D.S. (1993) Establishing retention periods for electronic records, *Records Management Quarterly*, April.

STROM, D. (1994) Who owns your e-mail messages? 'Netiquette' for business, *InfoWorld*, **16**(20), 16 May, 45.

THOMPSON, J.A., K.B. DeTIENNE and K.L. SMART (1995) Privacy, e-mail and information policy: where ethics meets reality, *IEEE Transactions on Professional Communication*, **38**(3), 158-164.

ULRICH, W. (1990) Rights of privacy in e-mail, *Los Angeles Times*, 7 September, D3.

WEIGNER, K. (1992) The trouble with e-mail, *Working Women*, April, 46.

The author

Pat Gannon-Leary

Dr Pat Gannon-Leary is a qualified librarian with a PhD in communication studies. She worked for 12 years at the University of Sunderland library in a number of posts and spent a year in the USA at Murray State University: she is currently employed at the University of Huddersfield Library as User Services Manager. The opinions expressed in this article are her own and do not represent those of her employer.