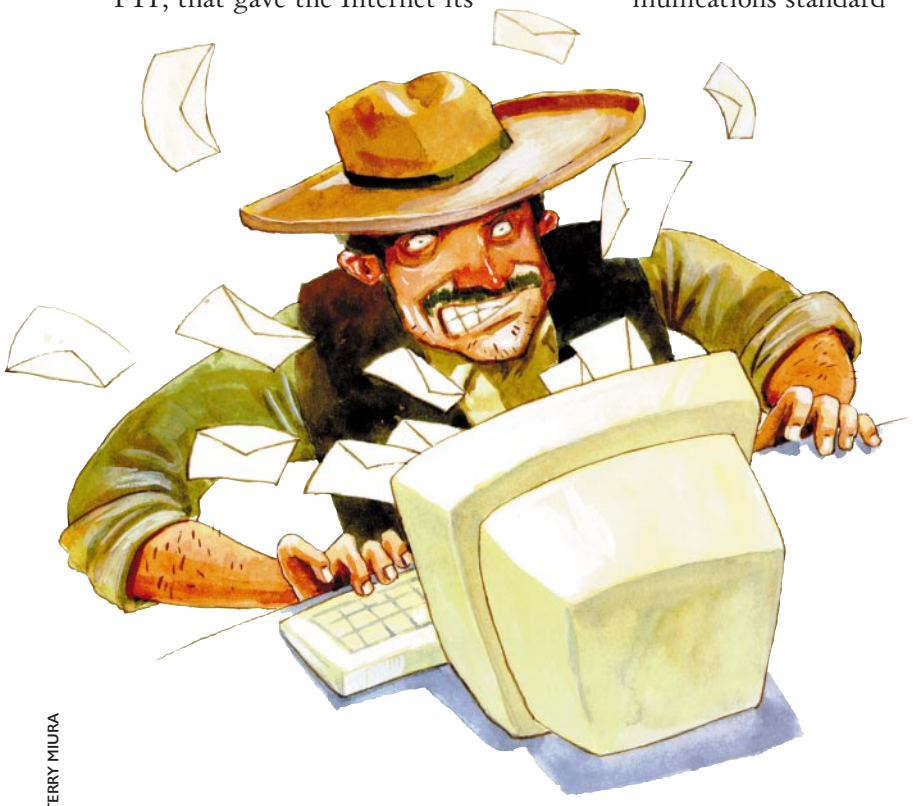
Hal Berghel

Email—The Good, The Bad, and The Ugly

Electronic mail has become the unexciting and mundane electronic communication medium we love to hate. It wasn't always that way. Hate is a fairly recent emotion.

Email has been with us in one form or another since the earliest days of computer networks and bulletin board services. From inauspicious beginnings, it became one of the three "killer apps," along with Telnet and FTP, that gave the Internet its momentum. Since the early 1980s, the popularity of the Internet and email have surged together.

Since the 1970s, email has evolved into the communication tool of choice for information technology academics and professionals. By the 1990s, the popularity and ubiquity of email throughout the rest of academia and high-tech industry, established it as a communications standard within those areas as well. It appears likely that the current wave of online service providers will soon extend this standard to the rest of the network-connected world.



TERRY MIURA

As email has evolved, we have come to surprisingly limited consensus regarding the best and worst uses of the technology, and whether it can ever overcome its weaknesses. In this column, I try to summarize what seems to me to be some interesting aspects of email, particularly as it relates to the phenomenon of information overload and some thorny privacy issues.

The Good

Some of the technical advantages of email over communication alternatives were obvious early. Among them:

- Email can be as fast as needed. As a network medium, email disposes of transmission delays imposed by geographical distance.
- Email, like post and unlike other electronic communication, is both asynchronous and half-duplex, and thus does not require scheduled, endpoint-to-endpoint connectivity. Sender and receiver can interact with their message autonomously and without distracting cross-talk.
- Email is a digital medium that

IT REMAINS TO BE SEEN HOW MUCH SERVER-SIDE RIGOR will be built into such future mail protocols as Internet Message Access Protocol.

(in principle) makes it amenable to the full range of computer-based tools and applications available on the desktop, most noteworthy file management tools.
- Email enables users to schedule interrupts. Should one feel the need for interruptions, bells, whistles, and sundry other annoyances are only a setup toggle away.
- Email is both paperless and archivable by default.
- Email can be efficient and convenient in the context of desktop automation. The efficiency derives in part from the fact that both sides of email communication may be completed in isolation—one doesn't listen to the other party.
- Email appears to be free, or at least cheap to the user. Such appearance is illusory, of course, as free lunches are as hard to find in cyberspace as anywhere else. But the cost of network connectivity, making email the luxury it really is, is either borne by the taxpayer and employer (as with direct Internet connections) or bundled with other online services. As a result, it's difficult at this point to put a price tag on the value of the service.

Other advantages were revealed through use:

- Email is a time manager's dream come true—users have virtually complete control over their end of the communication partnership.
- Compared to communication alternatives, email turns out to be on the low side on bandwidth but in some contexts makes up for low bandwidth with considerable velocity. This makes it especially useful for short, focused communication, less so for lengthy diatribes.
- Email's double-blind processing—the sender doesn't know how a message is being handled and the receiver doesn't know the circumstances under which the message was sent—creates a kind of processing hierarchy at both ends according to the degree of automation applied. Senders can personally craft the message, delegate authorship, prepare from a boilerplate, and so forth, while receivers can delete without reading, read without responding, skim with or without response, and so forth.
- Email has definite social implications, although no general agreement on what they are.

The following are some views on usage that seem to have currency in the literature:

- In the absence of such interpersonal communication cues as gestures, intonation, eye movement, and so forth, email communication is more easily misinterpreted than might have been predicted in the 1970s. This phenomena added a new term—flaming—to our vocabulary.
- Email can remove social distance as well as geographical distance as it suppresses status cues. This is both a blessing and a curse.
- Email can support and sustain communities of interest.
- Email can be a weapon in organizational politics.

To be sure, a healthy body of literature speaks to email's other social effects—in some cases, inconclusively. For example, there is evidence email communication may produce and ameliorate anomic communication partnerships; email contributes to and helps overcome users' feelings of isolation; email is sometimes impersonal and sometimes not; and email may increase and decrease sociability in communication. All are important areas of study and equally beyond present purposes.

Because of these benefits, the popularity of email soared. But this growth is not without discomfort.

The Bad

As with any new technology, email has a darker side. More than an inexpensive communications medium, email may also be

an individual and organizational resource drain. Here are some drawbacks:

- Email may lead to communication slavery. My law of digital sinkholes holds that once the foot is in, the ankle and leg soon follow. In this case, conscientious, established emailers have nowhere to hide once their email addresses get through—and email always (almost) gets through. One normally can't ignore email, as one ignores the telephone, without the potential of repercussion—even if it's unsolicited and from a stranger. Few among us can afford the luxury of disconnecting ourselves. (Pre-eminent computer scientist Donald Knuth is a notable exception in this regard—see, www-cs-staff.stanford.edu/~knuth/email.html.)
- The convenience of email encourages abuse at the interpersonal level. Since email may easily circumvent established organizational information routes, and since there is no cost to the sender associated with transmission, the temptation to harangue a stranger is sometimes too much to ignore.
- Email extensions encourage irresponsible mass-mailings. Alias and distribution lists make email bombing and spamming inevitable. Like telephony, the advantages of email are most evident as point-to-point communication; and like hardcopy junk mail, the disadvantages of email are most evident when it comes to "broadcasting" due to its inherently intrusive nature.
- There are few effective tools for adjusting email in-flow to what Peter Denning calls "personal bandwidth." It is interesting to note that not much has changed since Denning made this point in 1982.

Denning set forth two fundamental requirements for email: there must be special paths for urgent, certified and personal email to arrive, and all other paths must be filtered. Denning also suggested that these two requirements might be satisfied by a combination of the following:

1. Content filters that scan incoming mail messages and message-headers, and store, route or delete accordingly;
2. Message prioritization based on a combination of an "importance" number determined by sender and a "bias" number for each sender determined by the receiver;
3. Separate, unlisted, private mailboxes whose address is controlled by the owner;
4. Special forms of delivery for certain categories of email so messages from privileged authors (perhaps identified by special keys) are handled differently;
5. Hierarchical mailbox organization corresponding to the organization's normal communication paths so email cannot circumvent sanctioned information flow; and
6. Threshold reception that assigns a cost to potential senders for the delivery of the each email—if the sender is unwilling to pay the cost, the email is not delivered.

We observe that modern email systems support only (1) through (3)—and even then it's a stretch. Message "scanning" by email programs is rudimentary by natural language processing standards, and the prioritization algorithms are hardly as robust as Denning would like. One might actually extend Denning's suggestion to include the requirement that prioritization schemes be intelligent and self-training. Even (3) is difficult to achieve from what I see as organizations post their employees' email addresses in online directories.

Requirements (4)–(6) still seem a long way off. The modern trend toward Post Office Protocol (POP) clients seems to work against these goals since they seem most amenable to server-side solutions. It remains to be seen how much server-side rigor will be built into such future mail protocols as Internet Message Access Protocol (IMAP).

The Ugly

The dangers of email do not end with information overload. In addition, the technology itself—at least as it is used—presents us with a new technological challenge and a social dilemma. Both of these will be of considerable importance to the computing communities of the near future.

The first challenge, and likely the easier to deal with, is security. Modern email clients support "attachments" foreign (to the emailer) data files, multimedia files, or executables. Such files are converted to ASCII, attached to email, transmitted and converted back again by the receiving client. The problem is with

the transmitted binary, executable files and represents a fairly significant security hole and a potential source for a new wave of computer viruses.

Email virus scanners are available for clients (e.g., MIMEsweeper, www.integralis.com; and Webscan, www.mcafee.com) and servers (Virus Wall, www.antivirus.com and WebShield, www.mcafee.com). Of the two methods, the client-side approach has a decided advantage in that the detector could conceivably spawn an existing, third-party antivirus utility, thereby avoiding much reinvention. The server-side approach has the theoretical advantage of not allowing infected mail onto the client in the first place.

Ill-behaved executables are another matter. An illustration of this problem's difficulty is found in the Java developers' struggle to implement the details of static type checking for applets. A likely first pass at email security might be to follow the lead of Web client developers and restrict execution to hobbled programs (e.g., applets), but even this has proven only partly successful as it admits system penetration by type-confusion attack.

Though the second challenge is not technological, it may have the most serious social costs. This is the challenge to find a balance between an organization's need to control its work force and the individual's right to privacy.

The email privacy issue came to light recently when employees began to discover their email was read by employers. In one case, when an employee of Pillsbury sent what he thought was a private email communication to a co-worker labeling Pillsbury as "back-stabbing bastards," he was fired for "inappropriate and unprofessional comments."

In subsequent litigation, it turned out that privacy of interpersonal email was not one of Pillsbury's corporate guarantees. The Philadelphia Federal District Court judge ruled that even if the company had made such a promise, reading employees email would not have "tortiously invaded" their privacy. This leaves open the question of balance between a company's right to insist its computer and network resources are used for company business and employees' rights to free expression.

Patrice Duggan Samuels, who covered the story for the *New York Times*, reported on the following corporate policies as of a year ago:

Intel. Email is monitored to ensure employees are not engaging in personal activities on company time.

Kmart. All email messages are subject to review. Personal use of email is considered a breach of company resource policy possibly resulting in denied access to the company computer system or termination.

Epson. Email is considered company property and subject to review, printing, storage, and dissemination by management.

Apple. No corporate policy.

It appears companies are reading employees email with increasing frequency, in turn producing a flurry of litigation. To mitigate against this, formal policies have been proposed, like this boilerplate policy for corporations provided by The Society for Human Resource Management: "I am aware that the company reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the company's email systems at any time, with or without employee notice, and that such access may occur during or after working hours."

From the user's perspective, perhaps the next step is email encryption. It might be that email privacy litigation of the next century will involve corporation's rights to insist on a back door key to the employees encrypted email.

Issues in Balance

Not only does email, our seemingly innocuous communications tool, have social implications we don't fully understand, now it appears to have legal ramifications as well. The legal is even more difficult to understand than the social.

Imagine a continuum between absolute employee privacy rights on one end and absolute employer's rights on the other. Since the extremes aren't viable (no company should have the right to put video cameras in the restrooms, and no employee should have the right to refuse to document large reimbursement claims), society needs to find a balance it can live with.

But where would employers placing employees under home surveillance fit? Is that closer to the "unacceptable invasion of privacy" end or the "necessary for

the operation of the organization" end? How about requiring polygraphs as a condition of continued employment—and over what range of questions? How about eavesdropping on employee telephone conversations? Taken in this context, the email question may be merely the latest incarnation of the ages-old conflict between workers' rights and those of the corporation.

What makes email different? Here are some distinctions:

- Email uses company computer systems. From a technical point of view this seems to be a red herring; company telephone systems also transmit (audio) information from and between the same group of employees. On this account, WAV or AU email attachments are not private, where as the same audio information would be private if transmitted by phone.
- Email is more persistent in the corporation while telephony is more ephemeral. Is that right? Isn't most email intended to be as temporary as telephony. Indeed, as we explained two advantages email has over voice communication are (a) it is often quicker to type-and-send missives than to connect telephonically and (b) the exchange is more likely to remain focused and less prone to gossipy digressions than voice communication. Further, voice mail can be as persistent as email.
- An email box is like your desk drawer or company locker where there is no expectation of privacy. If this doesn't set up an adversarial relationship between employer and employee, nothing will.

I have another hypothesis: Could it be the technological imperative has reared its ugly head once again. Maybe employers read employees' email because they know how to do it without being obviously intrusive and without being detected. The question that society has to resolve is whether eavesdropping is somehow more ethical if it's digital.

Conclusion

In the end, we have yet to fully appreciate email for what it is—its status as a favored communication medium of the network is secure. But it is becoming increasingly evident that, like its communication technology ancestors, it comes with penalties. Just how many and how important, are yet to be determined.

A few things seem clear: First, increasing the volume of information is not necessarily a social good. To paraphrase Denning, increasing verbiage without increasing the number of good ideas doesn't get us very far. Since we have no objective comparisons of the efficiencies of email offset by the economic penalties of the unnecessary time hits and distractions, it is difficult to estimate the extent of productivity gains achieved by email. It would be useful to question the degree to which alleged email efficiencies are real or imagined. When we claim email efficiency, are we reporting statements of fact or the cognitive arrogance that derives from unreflective dependence on the technology? As the saying goes, "To a person who only owns a hammer, everything appears as a nail."

Another obvious fact is that email is a wonderful testbed for researchers. At once they have an opportunity to investigate the modern standard for on-demand communication partnerships and interpersonal (though not-in-person) digital communication. As we advance into such new technologies as Internet telephony and networked conferencing, we may yet see this testbed as email's greatest contribution. C

HAL BERGHEL is a frequent contributor to the literature on cyberspace. Visit his Web site at www.acm.org/~hlb/.

Further Reading

A good place to begin to look at the negative aspects of email communication is M. L. Markus, "Finding a Happy Medium: Explaining the Negative Effects of Electronic Communication on Social Life at Work," *ACM Trans. on Info. Syst., 12*, 2, pp. 119–149. Peter Denning's prescience with respect to electronic junk mail is evident in his "President's Letter," "Electronic Junk," *Communications*, Mar. 1982, pp. 163–5. Denning's exchange with his critics in the "Forum" the following June is also worth a look. An overview of the email privacy issue may be found in the article, "Corporate Electronic Stationery," in the May 12, 1996 *Sunday New York Times*.

If you're interested in this topic and have ideas on email, visit my "Email: Good, Bad and Ugly" home page at www.acm.org/~hlb/email_gbu/. Here's a chance to add something to the online literature. Include your name for credit.