# HIDDEN DANGERS OF ELECTRONIC MAIL

John M. Carroll
Computer Science Department
University of Western Ontario
London, Ontario

## ABSTRACT

Electronic mail is destined to change profoundly our way of life. On the positive side, it will bring about cheap and dependable instantaneous interactive communication around the block or around the world. On the negative side, it can facilitate espionage, vandalism, libel, impersonation, fraud, plagiarism, breach-of-trust, and invasion of privacy. Moreover, to protect against these dangers could bring about a frightening loss of personal freedom.

# LES PIEGES DU COURRIER ELECTRONIQUE

## RESUME

Le courrier électronique est appelé à modifier notre comportement social. D'un côté, on met en place un moyen interactif de communication instantané, fiable et peu coûteux qui nous permettra de rejoindre aussi bien notre voisin à son domicile qu'en voyage à l'autre bout du monde. D'un autre côté, on facilitera l'espionnage, le vandalisme, la diffamation, la contre-façon, la fraude, le plagiat, l'abus de confiance, l'ingérence dans la vie privée. Bien plus, les solutions pour se protéger de ces dangers font brandir le spectre de la perte des libertés individuelles.

# HIDDEN DANGERS OF ELECTRONIC MAIL

John M. Carroll

Electronic mail is coming on apace. In the United States, the Postal Service estimates that in 1982 it will handle seven million pieces of Electronic Computer-Originated Mail (ECOM). This is the immediate precursor of electronic mail. Letters composed on user-owned computer terminals can be sent to one of twenty-five post offices. There, a hard copy is printed and for twenty-five cents delivered to the recipient by conventional first-class mail. The Postal Service estimates that by 1985, it will be handling about seven billion pieces of electronic mail annually,. By then it expects to have implemented completely electronic mail wherein letters will be reproduced directly on user-supplied computer terminals.

Actually, electronic mail in various forms has been around for a long time. Record communications have long been available to users of the Bell System's teletypewriter exchange (TWX) or Canadian National/Canadian Pacific Telecommunications TELEX networks. In these systems, messages were originated and received on carrier-owned equipment installed on the customer's site. Usually these communications were handled by operators trained in network protocol; and routed to the ultimate recipient by internal mail with inevitable delays. The reasons why each user did not have an individual terminal and why incoming messages were not fed into customer computers were reasons of policy, convenience and economics, not technical limitations.

With the cooperation of the recipient, any person with access to a computer terminal or microcomputer has the capability to store a message in a comptuer selected by the recipient. Voice-grade telephone lines of the public switched network adequately handle most slow and moderate-speed communications. You can even communicate over public or private radio links. High-speed and cheaper communications are available if one of the parties is a subscriber to Trans Canada Telecommunications Service's DATAPAC service or CN-CP's INFOSWITCH. One of the principal technological advantages of computer-switched networks is that messages can be stored in network computers so they can be delivered during working hours in distant time zones (store-and-forward). This storage also ensures there is a back-up copy in the event of line failure or undecipherable transmission error and provides independent third-party confirmation that a message was sent.

Users of remotely accessed resource-sharing computer systems (time sharing) have long been able to send messages to each other and sometimes to users of systems other than their own. Sometimes it was necessary to make program modifications to systems software. Now several popular computer operating systems have built-in provisions for handling electronic mail.

Probably the first major experiment with the use of electronic mail was the ARPA-NET. The experiment was sponsored by the Advanced Research Projects Agency of the U.S. Department of Defense. The members of the network included the Pentagon, the more research-oriented establishments of the DOD, and several universities with defence research contracts. Much of what we think we know about the sociological implications of electronic mail has been extrapolated from experiences reported by users of ARPA-NET.

The major difference between electronic mail in its earlier incarnations and what we are witnessing today, is of accessibility. The Institute for Research on Public Policy reports that in 1978 there were 56,000 TELEX and TWX message terminals and 8,000 facsimile terminals. (Facsimile is a technique for transmitting graphical information by telecommunications.) These populations are expected to grow to 70,000 and 28,000 respectively by 1985 -- hardly an earth-shaking market explosion.

However, the significant growth lies in other areas. Communicating word processors, computers and data terminals can all be considered candidates to become originators or recipients of electronic mail. In these three categories the IRPP figures are:

| | 1978 | 1985 |
|---|---|---|
| Communicating Word Processors | 1,000 | 10,000 |
| Computers | 18,000 | 150,000 |
| Data Terminals | 250,000 | 700,000 |

At two and a half users per terminal, one could anticipate that 2.15 million Canadians will, by 1985, have potential business access to electronic mail. Not all computers and terminals will make use of this capability, however. Many will be dedicated to programmed data collection such as on-line banking, airline reservations, and point-of-sale terminals. It seems reasonable nevertheless to forecast that by 1985, nearly all large and medium-sized companies, government agencies, research laboratories, universities, and colleges will have access to, and be using electronic mail, not to mention some 20,000 computer hobbyists and a like number of self-employed professionals.

The first publicized negative indication associated with electronic mail was reported in February 1982 when it was revealed that some unidentified person had unlawfully penetrated the ARPA-NET

access port at Stanford University in Menlo Park, California and had used this access to vandalize files at the Digital Equipment Corp. in Newton, Massachusetts. Sources at Stanford, DEC and the Pentagon were understandably reluctant to disclose how the penetration had been accomplished or what, if any, classified information had been compromised. How the penetration was made and what was subsequently done is unimportant here. What is important is that electronic mail creates unprecedented opportunities for unauthorized penetration of confidential files at unlimited distances.

Another problem associated with electronic mail is one that bankers have wrestled with for some time. This is the problem of the electronic signature. Short of using public-key encryption, a technique still very much in the experimental stage, there is no known way that any electronically transmitted message can commit its author the way a signed letter can. Even the point of origin may be in doubt. Computer terminals have provision for a so-called "here is" chip or card that automatically identifies it to the host computer, but there are no identification standards and no legal requirement that such an option be implemented. Home computers can be used as computer terminals. They usually don't identify themselves, and besides, a knowledgeable technician can easily modify a terminal to transmit any misidentification signal desired. Communications carriers can trace calls and have successfully done so, both in the Dalton School affair (a 1980 case where eight thirteen-year-old New York schoolboys penetrated, via TELENET and DATAPAC, the files of Canada La Farge Cement in Montreal and the Scott consultancy (in Ottawa) and in other heretofore unpublicized cases. Carriers are not anxious to play detective, and in some cases are unable to do so.

One of the first uses of electronic mail was for researchers to expose papers in preparation to critical comment by their peers at distant laboratories. At least one former user of ARPA-NET claims that other users pirated his research results and anticipated publication of his papers. Therefore, confusion of authorship is already one of the negative consequences engendered by electronic mail.

Complaints about other unprofessional conduct by users of ARPA-NET include reports of unsigned obscene comments about fellow scientists and their work, unauthorized recruiting, malicious modification of research data, destruction of files and messages from other users, and unethical use of privileged information in bidding for government contracts.

Computer science departments have used internal electronic mail to post grades, set homework assignments and circulate programming exemplars. Ever since the shortage of computing resources and instructional personnel made it necessary to hold merit competitions for places in computer science programs, there have been reports of grade switching to alarm and discourage fellow students and tampering with assignments and exemplars to frustrate their progress.

Electronic mail can also facilitate invasions of privacy. A mammoth wiretapping effort like the one undertaken by the British Security Service is more easily conducted against record communications in the store-and-forward mode than against voice telephone communications where the ultimate upper bound is set by the lack of stenographers to transcribe the tapes. It's far easier than opening mail too; and there are no nosy posties to blow the whistle.

Although it is not generally known, the monitoring instruments used by CN-CP and TCTS to ensure high-quality transmission are also superb digital wiretapping equipment.

Unfortunately, any measures that could be taken to prevent espionage, vandalism, libel, impersonation, fraud, plagiarism, breach-of-trust, and invasion of privacy by electronic mail, would themselves invade the privacy of individual citizens. One recoils at the thought of assigning every user of electronic mail a personal identifying number or procedure to be programmed on a chip laminated into a card and carried at all times; mandatory licences for home computers; having to pay a fee every year for a new "here is" chip manufactured in Milhaven Penitentiary; random stops and home searches to enforce these laws; continuous computerized tracing of data communications; background investigations of telephone employees; and fortress-like central offices. It would take this, and more, to counter the hidden dangers of electronic mail.

I'm not sure it's worth it.