# Technology and Public Policy: Privacy and Security in the Decentralized Network

by Marc Rotenburg



Columbia Institute for Tele-Information
Graduate School of Business
Columbia University
809 Uris Hall
New York, NY 10027
(212)854-4222

# Technology and Public Policy: Privacy and Security in the Decentralized Network

Marc Rotenberg



Columbia Institute for Tele-Information
Graduate School of Business
809 Uris Hall
Columbia University
New York, New York 10027
(212) 854-4222

"Technology and Public Policy:
Privacy and Security in the Decentralized Network"

Marc Rotenberg,* Director
CPSR Washington Office

Private Networks and Public Objectives
Columbia Institute for Tele-Information
Columbia University
New York, New York
September 25, 1992

"To think that a bit of paper, containing our most secret thoughts, and protected only by a seal, should travel safely from one end of the world to the other other, without anyone whose hands it had passed through having meddled with it."
- Ralph Waldo Emerson, American philosopher and poet (1803-1882)

Privacy and security raise two distinct sets of issues for the design and management of decentralized networks. Privacy refers generally to the protection of personal information. Security refers generally to the protection of network facilities.

In the first instance, we need to know what type of information is collected, when it may be disclosed, whether there is a duty to keep the information confidential. Is the information public or private? For a communications network, we would consider both the content of a communication and the record of a communication. With electronic mail, for example, there is a privacy interest in both the content of the message and the details regarding the transfer of the message: the identity of the sender, the identity of the recipient, the date the message was sent, and its subject matter. In many instances, the protection of this transactional data is as critical as the protection of the message itself.

---

* Adjunct professor, Georgetown University Law Center; former counsel, Subcommittee on Technology and Law, Senate Judiciary Committee; A.B., Harvard College, J.D., Stanford Law School; member, United States Supreme Court bar. Contact: CPSR Washington Office, 666 Pennsylvania Ave., SE, Suite 303, Washington DC 20003, 202/544-9240 (tel), 202/547-5481 (fax), rotenberg@washofc.cpsr.org (email).

With security we look at a different set of interests: the protection of computer systems and network facilities, the prevention of unauthorized use, and the risk of the deliberate denial of services. In the security world, there are also different measures for determining the adequacy of protection. At the intelligence end of the spectrum the emphasis is on access controls and user authentication. Who is using the system, why, and does this person have proper authorization? At the civilian end the focus shifts to the reliability of services and the integrity of data. Can we ensure that the information will be available when it is needed? Will it be accurate and reliable?

In most instances the two goals of privacy and security will be complimentary; in some cases they may be at odds. I suspect that one of the most difficult issues that organizations in the decentralized network environment will confront will arise when these two goals conflict.

## PUBLIC POLICY

There are a wide range of policies and laws for computer security and computer privacy. They include simple codes of conduct, elaborate organizational policies, professional guidelines, and legal obligations based in federal and state law. At the federal level, there are many privacy laws, but only a couple of laws that might be properly considered computer security laws.

### Security and Computer Crime

The Computer Fraud and Abuse Act, passed in 1984 and amended in 1986, sets out criminal fines for a variety of offenses. These include the use of a computer system without authorization, or exceeding authorization, to obtain financial information, to commit a fraud, to alter, damage or destroy information, to prevent the use of a system, or the trafficking in stolen passwords.

There was an interesting application of the law in a 1988 case involving a Cornell student who released a computer worm that travelled across the Internet. The district court in Syracuse found that the perpetrator had exceeded his authorization by using the network facility in this manner. It also found that it was not necessary for the government to show that the student intended the harm which resulted, only that he intended to use the network in an unauthorized manner. The Second Circuit agreed, leaving many with the belief that the scope of the law was very broad.

As a practical matter, the CFAA may have little bearing on private networks. If the computer system does not fall

within the Act's scope, the law may not apply at all. CFAA is also likely to be invoked only when there is substantial harm to an organization. There is understandable reluctance to make the law so broad that it becomes simply a "computer misuse" statute.

The second area of federal security policy covers computer security authority for government computers. The Computer Security Act of 1987 placed the National Bureau of Standards, now the National Institute of Standards and Technology, in charge of civilian security for the federal government. This may be significant for the operation of private networks because one of the reasons for the transfer of authority from the National Security Agency was to ensure that federal security policies were more closely aligned with civilian needs.

The Computer Security Act also established the Computer System Security and Privacy Advisory Board. Its twelve member board includes members of computer firms, officials from government agencies, and private consultants. It is responsible for overseeing the implantation of security and privacy policies for federal agencies.

It is worth noting that one of the issues that has most interested the Security and Privacy Advisory Board are the policies surrounding cryptography, a technology that both enhances security and privacy. The widespread availability of cryptography has raised concerns in the law enforcement and intelligence communities that wire surveillance may become more difficult in the future. For this reason, both the FBI and the National Security Agency have sought to restrict the use of cryptography. However, businesses have argued that current restrictions already impose significant burdens on network users that are attempting to incorporate more advanced privacy-enhancing technologies. The Advisory Board is currently considering the development of a new cryptography policy that may better serve commercial needs.

Privacy

Privacy laws cover a range of information systems from the records of government agencies to banking records, credit reports, and even video rental records. Virtually every privacy law in the United States is based on the premise that an organizations has an obligation to restrict the disclosure of personal information. Personal information should only be disclosed in certain circumstances. These circumstances include disclosure necessary for the conduct of business and the rendering of services, for civil suits, and criminal warrants, or when the consent of the record subject is obtained.

For our purposes, the most important privacy statute is the Electronic Communications Privacy Act of 1986 (ECPA). ECPA protects electronic communications in transit as well as stored electronic messages. This law amended the wiretap statute of 1968 and extended the protection for aural communication to digital communication. The federal wiretap statute, which places certain restrictions on the disclosure of communications, recognizes that service providers may also need to monitor communications to ensure network maintenance.

Privacy Within the Organization/Network

Perhaps the most difficult area of privacy law today is workplace privacy. The implications for private networks are clear. The question posed is a simple one: does an employee have a right of privacy in electronic communications in the workplace?

As as a starting point, the answer to this question is currently no. The Electronic Communications Privacy Act covers the exchange of electronic mail across public networks, but it does not provide protection to messages that travel through private networks. Tort law, another source of protection for workplace privacy, offers relief against intrusions that are "highly offensive" to a reasonable person, such as the placement of video cameras in a rest room, but is not likely to succeed where the harm is simply the loss of privacy in electronic mail.

Thus organizations operating through private networks will likely develop their own policies regarding the privacy of electronic communications. The task will be complicated, however, when messages travel through public networks.

## SIGNIFICANCE OF DECENTRALIZED NETWORKS

Decentralized networks will confront overlapping and at times conflicting policy guidance when they confront federal laws on security and privacy. The Computer Fraud and Abuse Act covers "federal interest" computers, information stored by financial institutions and medical records. Privacy statutes are more complex still since they tend to focus on the storage and release of data, rather than the disclosure of data "in motion."

An effort currently underway by the Organization for Economic Cooperation and Development has attempted to set out a series of general principles for computer security that could be applied. If successful, the impact of the OECD Computer Security Guidelines may rival the 1981 OECD policies on Privacy and Transborder Data Flow, which are now followed by the majority of OECD nations.

Even if the OECD successfully isolates key privacy and security principles, certain issues are likely to move to policy forefront in the next few years.

1. Impact of European privacy law on Data Transfers from the United States

One of the closely watched issues on the privacy front is the potential impact of the EC draft Data Protection directive on data transfers originating in the United States. Under the EC Directive, countries that fail to adopt "equivalent" or "adequate" (the terms are changed as the resolution is debated) privacy standards may face restrictions on the transfer of personal data to Europe.

2. Impact of differential levels of privacy protection

The development of multiple, decentralized networks may lead to inconsistent levels of protection. Interoperability for network communications remains an important goal, but where networks vary in technical standards or policy guidance, problems may arise.

3. Significance of transactional data

One of the areas where technology has clearly outpaced the law is the failure of privacy law to recognize the growing importance of transactional data. While message content continues to receive the highest level of protection, transactional data receives substantially less protection. Law enforcement agents may, for example, obtain telephone billing information from telephone companies merely upon the presentation of a subpoena. The Supreme Court has held that in this circumstances, the customer has no legal stake in the disclosure of the information. The duty then falls on the service provider to determine when and under what circumstances to disclose this information.

The increasing availability of transactional data in the digital network is likely to increase pressure to develop protections for this data. One of the interesting opportunities for resolving privacy concerns may be in the design of networks which simply do not generate extensive collections of transactional data. Telephone cards are widely used in Europe, Japan, and Australia. They are cash-based, debit cards that may be freely sold and exchanged. There is no link to a particular account or to a particular user. The use of such cards should be pursued in the United States.

4. Law Enforcement Investigations

One area that has moved rapidly to the forefront of discussions about network security and privacy is the concern expressed by the Department of Justice that new technologies, including encryption, fiber networks, and packet-switching will create obstacles to law enforcement investigations. The practical problem is that law enforcement may not be able to execute court ordered wire surveillance. While the legislative proposal to give the Department of Justice the authority to set communication standards to ensure the continued viability of network surveillance has stalled in the United States, a similar proposal was acted upon favorably last year in France.

The long-term consequences of the Department of Justice Proposal could be substantial for network security and privacy. Arguably, both interests could be diminished if the Department of Justice is permitted to redesign the network to facilitate wire surveillance.

References:

Commission of the European Communities, Proposal Concerning the Protection of Personal Data in the Context of Public Digital Telecommunication Networks
Draft directive on telecommunications policy.

David Flaherty, Protecting Privacy in Surveillance Societies (University of North Carolina, 1989)
A comparison of privacy regulation in Canada, France, Germany, Sweden, and the United States.

David Linowes, Privacy in America (University of Illinois, 1989)
Includes an extensive survey on privacy practices and policies for Fortune 500 companies.

Wayne Madsen, Handbook of Personal Data Protection (Stockton Press, 1992)
An extensive compilation of national and international privacy and data protection laws.

# Privacy and Security in the Decentralized Network

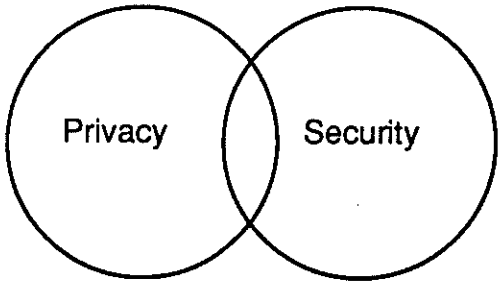
"Private Networks and Public Objectives"
Columbia Institute for Tele-Information

Columbia Business School
September 25, 1992

Marc Rotenberg, Director
CPSR Washington Office



## Privacy and Security



# Workplace Communications

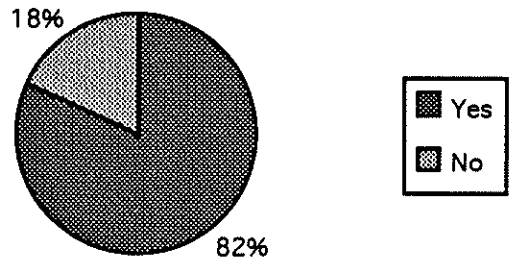
- Interpersonal
- Written notes
- Telephone
- Computer e-mail



# InformationWeek Survey

- Bruce Caldwell, "E-Mail Privacy: A Raw Nerve for Readers," July 30, 1990
  - > "The company does not provide computers and networks for personal use!"
  - > "Don't use company equipment to do things you don't want the company to know about."
  - > "Users should have a protected password and an indicator that would let them know if someone has gone into their E-mail."

## Survey: Expectation of Privacy

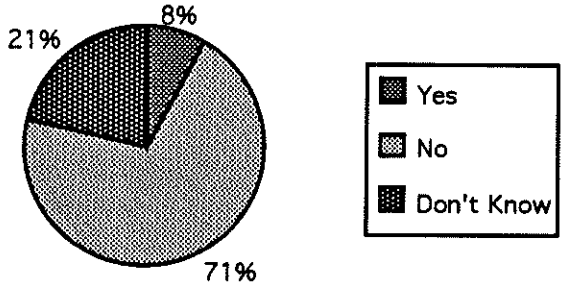



"Would you consider it a violation of your privacy if your employer read your electronic mail without your consent?"

Source: InformationWeek, July 30, 1990



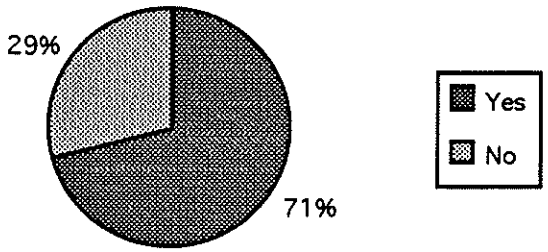
## Survey: E-Mail Policy




"Is there a formal E-mail privacy policy in your organization?"

Source: InformationWeek, July 30, 1990

# Survey: E-Mail Privacy

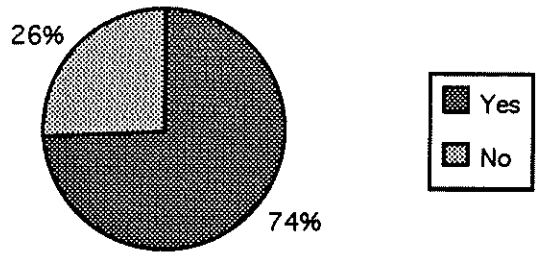



"If there is no written E-mail policy, is it assumed that E-mail is private?"

Source: InformationWeek, July 30, 1990



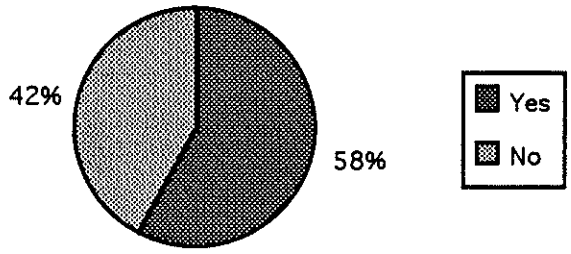
# Survey: Is Law Appropriate?




"Should employers be prevented by law or policy from reading employees' electronic mail?"

Source: InformationWeek, July 30, 1990

## Survey: Need for Exceptions

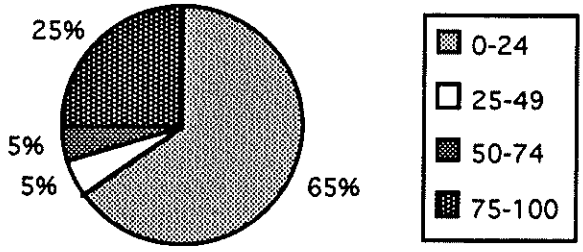



"Should there be exceptions for pressing business needs?"

Source: InformationWeek, July 30, 1990



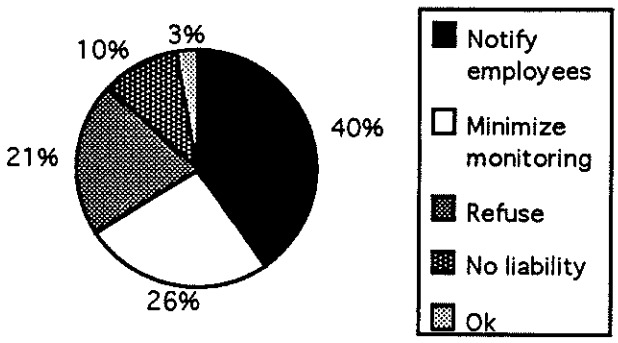
## Survey: Personal E-Mail Usage




"Percentage of E-Mail Considered Personal"

Source: InformationWeek, July 30, 1990

# Survey: Employee Monitoring




"What would you do if asked by your employer to monitor electronic mail?"

Source: InformationWeek, July 30, 1990



# Workplace Privacy I

Office of Technology Assessment (1987)

- "4 to 6 million office workers have their work measured by computers"
- "There are strong arguments that the present scope of computer-based monitoring is only a preview of growing technological capabilities for monitoring, surveillance and worker testing on the job."
- "If this is the case, then there may be a need for a new balance between workers' rights to privacy or autonomy in the workplace and management requirements for information."

# Workplace Privacy II

- "[Computer monitoring] makes it easier to grade, time and set quotas. It's labor controlling but not labor saving." (Barbara Garson, *The Electronic Sweatshop* 1988)
- "Monitoring is the ultimate expression of lack of trust." (Karen Nussbaum, National Association of Working Women)
- Massachusetts Coalition on New Office Technology survey:
  - > 62% of respondents were not informed they would be monitored prior to hiring
  - > 3/4 say that monitoring lowers morale
  - > 80% say monitoring makes their job more stressful



# Workplace Privacy III

PROPOSED GUIDELINES

- Right to know about monitoring practices
- Right to due process safeguards
- Establishment of meaningful standards
- Incorporation of employee input in monitoring policy

Source: *The Electronic Monitoring of the American Workforce*, 9 to 5, Working Women Education Fund 1990

# Case Study: UCSD I

University Policy:

"Any use of an instructional computing resource, class account, or computer access privilege for other than the specific academic computing requirements of the class is not authorized. . . ."

"Files belonging to individuals are to be considered private property. For example, users should not attempt to gain access to the files or directories of another user without explicit authorization. . . ."

"Be aware that electronic mail and computer files are not private in any absolute sense. Administrators and operations personnel may have access to mail, files and accounts in the normal course of their duties."



# Case Study: UCSD II

INCIDENT

- Conflict between student and professor
- Professor searches student files alleging misuse of University resources

OUTCOME

- Student association adopts resolution on E-mail privacy
  1. Students' expectation of privacy and confidentiality
  2. Availability of less intrusive methods
  3. Establish E-mail privacy policy in consultation with students
- University considers new policy

# Transactional Data I

"No person not being authorized by the sender shall intercept any communications and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."

Federal Communications Act of 1934, section 605



# Transactional Data II

TRANSACTIONAL DATA

- Identity of sender
- Identity of recipient
- Data and time of message
- Message length

> Use in audit trails and system security

DATA MINIMIZATION

- David Linowes, *Privacy in America* (1989)
- Library record destruction policy
- Federal privacy law record destruction policy

# Protection of E-Mail

Technical Mechanisms

- Sealed envelopes
- Locked file cabinets
- > Encryption
- > Data minimization

Legal Mechanisms

- Legal sanctions
- Policies and practices
- Remedies



# ECPA

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 et seq.

- Extended wiretap protection to digital communication
- Analogy is sealed envelope
- Establishes rights for users of **public** e-mail systems (e.g. Prodigy, Compuserve, MCI Mail)
- Does not apply to federal agencies

# E-Mail Privacy Policy

1. Make policy known to users and uphold
2. Solicit user input
3. Protect fundamental expectation of confidentiality
4. Establish technical mechanisms to ensure privacy and security of communications
5. Establish clear guidelines for when E-mail may be opened
   - Maintenance of system
   - Specific illegal or unauthorized act based on particularized suspicion
6. Use least intrusive methods to maintain system and to allocate system resources
7. Minimize collection of E-mail audit data