

The invasion of privacy.

The considerable faith we place in computer based record systems may be unjustified.

Database disasters.

Darlene Alexander believed that she had a respectable credit record. A stolen credit history allowed an impostor to open accounts in her name and take out loans, with the result that Alexander is now stuck with a poor lending history and has little chance of gaining credit for a home purchase or other important purposes.

Michael DuCross was stopped by a police patrol car after he had made an illegal left turn. Records indicated that DuCross was wanted by the federal government for going AWOL from the Marine Corps at Christmas in 1969. Five months later, the charges were dropped after it was discovered that DuCross had never gone AWOL. Michael DuCross, lost five months of his life because of blatant database mismanagement.

A U.S. citizen's wallet was stolen by a criminal who subsequently adopted his identity. The thief was later involved in a robbery involving murder. Even after the confusion of identities had been discovered, the U.S. citizen was arrested five times in 14 months on the basis of the same incorrect data records.

The information mosaic.

Data is the basis of a complex web of data dependencies and symbiotic relationships.

To get the driver's license, a mortgage, or credit card, to be admitted to a hospital or to register of the warranty of the new purchase, people in the United States routinely fill out forms providing a wealth of facts about themselves. Little of it remains confidential.

The major players in this commercial information ecology are the three giant credit bureaus: TRW, Equifax, and Trans Union. Every month the big three purchase computer records, mostly from banks and retailers, that detail the financial activity of virtually every adult American.

The major enduring problem is the difficulty in detecting incorrect information. According to some reports, as much as 30 to 40 percent of the information contained in the databases of the big three is inaccurate.

Unfortunately, in the United States, a person applying for life insurance enjoys none of the privacy rights and protections of a person applying for credit. Given the growing interest of the insurance industry in recording genetic defects and other newly revealed medical information, one wonders how much further scope there will be for such errors and what their effects will be on people's lives.

Communications systems.

Caller ID has generated much heated debate, with opposing camps differing over which party should be protected from. Computer hacking might be curtailed by recording the numbers of unsuccessful logins via modem.

Privacy legislation.

Most countries have come to terms with the need to treat information as property. European guidelines indicate that data can only be obtained by lawful means and with the

data subject's knowledge or consent. Data subjects have the right to inspect any data concerning themselves as well as the right to challenge the accuracy of such data and have it rectified or erased by the collector.

Big brother.

The national security agency (NSA) is the epitome of what we have most to fear in terms of the invasion of individuals' privacy and covert control of people's lives. In 1971 the agency needed a high temperature incinerator capable of destroying at least six tons an hour or and not less than 36 tons in any eight-hour shift.

The FBI requested that it be given authority to set technical standards for the computer and communications industry. This case illustrates the classic to the war between the perceived role of the state to preserve law, order, and national security and the rights of individuals to fundamental democratic freedoms.

Encryption would make it substantially more difficult for the NSA to monitor overseas voice and data communications. It would become a nightmare for the organization if such practices caught on and became commonplace. *They already have!*

Clearly, a the possibility of any PC user, drug dealer, terrorist, or spy being able to defeat the power of the NSA with a humble MS-DOS machine is a bitter pill for the federal agency to swallow.

Are the costs of privacy greater than the benefits of squeezing drug trafficking out of existence? Is the damage visible on the streets preferable to the invisible, secret damage that surveillance could bring to society and its freedoms?

Information contained in databases as part of a mosaic in which individual pieces are innocuous but, when aggregated, allow a more complete picture to appear. The blueprint for an H-bomb in 1979 appeared in the *Progressive* magazine. All the information contained in the article was gleaned from unclassified data scattered throughout various scientific journals.

Surveillance societies.

In Asia there appear to be no qualms about embracing the Orwellian concept. The Thai government inaugurated a centralized database which includes a population identification number with a computer readable ID card with photo, name, address, height, thumbprint, parent's names, marital status, children's names, education, occupation, income, nationality, religion, tax return, and criminal record (if any).

Indonesia and the Philippines are considering adopting the Thai system.

The government of the Republic of Singapore has committed itself to a road tax system that works by monitoring car locations and levying an appropriate fee for road usage.

Computerized monitoring systems.

Some reports have indicated that up to 26 million Americans are having their work tracked electronically. Work performance of workers is being monitored closely with computer systems.

Wall Street has had to invest in surveillance technology that is designed to detect aberrant trading patterns. What kind of precedent will computer-based monitoring of employees set for other invasive practices?

We see perhaps the greatest threat to our privacy as: the removal of our rights to be treated as individual human beings and not as a Social Security number, a number plate, a credit history, or an insurance record.

We need to ponder the issue of what the application of computing to social processes means for the rights and freedoms of ordinary citizens. How can we ensure that our lives are not a litany of database errors? How can we ensure the proper functioning of a democratic society and adequate control of criminal elements and yet still maintain a society relatively free of surveillance?

The first step toward the resolution of any problem is to be aware of it.

Social Questions And The Internet.

The Net is being buffeted by forces that threaten to destroy the very qualities that fueled its growth. It's being pulled from all sides: by commercial interests eager to make money on it, by veteran users who want to protect it, by governments that want to control it, by pornographers who want to exploit its freedoms, by parents and teachers who want to make it a safe and useful place for kids.

History.

The Genesis of the Internet can be traced back to the ARPANET project of the Advanced Research Projects Agency of the Defense Department. The ARPANET became operational in 1969.

The National Science Foundation's NSFNET became the common backbone for all networks that constitute the Internet.

The Internet is heavily commercial, but also supplies other diverse uses such as e-mail and usenet newsgroups, and universal file transfer.

Some inadequacies of the Internet include insufficient mechanisms to guarantee privacy and security.

The Internet is the foundation of the Nation's emerging information superhighway.

Several pressing and vexing social and moral issues are connected to the usage of the Internet. These include the ability to remain anonymous while communicating in cyberspace, the civil liberties question, and the problem of universal access.

Anonymity in cyberspace.

Anonymity can sometimes promote free expression. Unfortunately, this sort of disguised communication can also lead to strange excesses. One can take on a whole different *digital persona* in the realm of cyberspace. It diminishes accountability and responsibility for one's actions.

Services such as "remailers", strip away in the original sender's name and any traces of his or her identity before "remailing" them on the Internet.

The American civil Libertarian's remind critics of "remailers" that the United States anonymity in cyberspace is protected a constitutional right to free speech.

Public policymakers must currently consider how to prevent abuses without imposing oppressive and counterproductive restrictions.

Free Speech in cyberspace

Restrictions on pornography in cyberspace are difficult to implement. How does society deal with this problem?

Libertarian groups are ardently opposed to any form of censorship.

Another school of thought proposes restraint of this material by the government. Critics of the government censorship point out numerous philosophical and practical problems with the solution. (i.e. the global nature of the Internet.)

Another school of thought maintains that offensive material should be restricted by users, organizations, and local communities.

Another issue of free speech in cyberspace entails hate speech.

The First Amendment right of free speech is obviously a fundamental principle of American democracy that should not be unnecessarily compromised.

Universal Access

The Internet is the information superhighway which is stimulating economic growth in our global economy.

Internet technology will give ordinary people more of a voice in politics.

Electronic access to the Internet will soon be as important as having a telephone.

Computer Professionals for Social Responsibility (CPSR) took the position that providing some level called "universal service" is both economically feasible and morally responsible. It is required to ensure that society does not become divided into the information-poor and the information-rich.

There is a notable gap between universal access and universal service. The larger question in all of this is the government's role in eliminating the fissure in society between the information "haves" and "have nots".

Should the government explicitly seek to close this gap or shouldn't be left in hands of the free market forces?

Computers, pornography, and conflicting rights.

Does one empowered individual who chooses to access information that may be considered offensive or threatening to another have the right to access it in a way that crosses beyond his/her own personal space and boundaries?

Information exists in graphic form; in text form; and some information consists of primarily sound. Sound can so readily permeate an environment that its potential for disturbance to others is obvious.

Reflections by a Ph.D. student:

“I should be able to finish my degree without having to feel uncomfortable and intimidated by those around me. When I look up from a my workstation, I see on a machine just two workstations away, pictures of nude females that I consider offensive and embarrassing.”

Does a university or college have any responsibility in this regard?

Such institutions have to proactively encourage individuals to think about the needs, rights, and values of others. By encouraging individuals to ask each other to be considerate of others' reactions to offensive material and to ask them to consider a less intrusive site for accessing it, is to encourage community sensitivity and social thinking.

Within each community, however, there are those who purposefully exposed others to material they may find offensive. Should we consider all such purposeful acts as harassment? No, what is offensive to one may not be offensive to another.

A young woman, though asked to stop sending electronic mail to an unwilling recipient, continued to send daily solicitations for lesbian sex, including increasingly intimidating descriptions of the acts to be committed, and the violence that would be involved. Should a university or college administrator intervene in these interpersonal conflicts?

This is not about an individual's right to access material. It is about another individual's rights to choose not to access or to be exposed to the materials.

It is a topic around which learning and teaching can be built. It is an opportunity to teach and reinforce essential liberties while empowering all individuals.

Computerizing the workplace.

Work still remains central to the lives of millions of people. The amount of leisure time enjoyed by the average U.S. citizen shrunk by a staggering 37 percent between 1973 and 1989. The average working week, including travel to work time, grew from 41 hours to nearly 47 hours.

There is no evidence to support fears of mass unemployment caused by technological change. Job losses would be more likely to result from the slow adoption of new technology rather than the too-rapid adoption.

There is little doubt that the computerization of factories and offices has led to the steady erosion of employment opportunities, particularly for less skilled manual workers and for clerical workers.

While the U.S. economy generated 18 million new jobs between 1982 and 1989 there was a net loss of jobs in manufacturing of more than half a million; and in the 1990 to 1992 recession, 1.1 million manufacturing jobs were eliminated almost overnight. By the year 2000, employment in the manufacturing industry as a proportion of the total U.S. labor force could be as low as 10 percent.

The majority of jobs in the future will be in low-tech or no-tech occupations such as cashier, receptionist, waiter, maid, hospital orderly, janitor, and security guard.

One trend is the growing tendency of U.S. companies to export routine data-processing jobs to countries with cheap labor by using the latest satellite and telecommunications technology.

There is wide agreement about the high-tech sector's inability to create large numbers of jobs in the future.

A U.S. economy dominated by services can continue to support real increases in income and wealth for a long time. Service sector jobs are generally less well paid, and they offer fewer fringe benefits. A quarter of the U.S. workforce is now in low-wage jobs.

In many instances, the 1990s young couple now takes home less money together than did the 1960 father alone.

The use of flexible manufacturing systems and computer-based systems in finishing, inspection, and production control after the mid 1990s will severely erode employment opportunities.

Quality and quantity of work.

Computers are transforming the office of the future into a kind of stressed out factory of the past.

Another issue causing considerable controversy at present is that of the computerized monitoring of employees. Computerized monitoring is constant, reliable, and cheap. Supervisors are no longer limited by what they can observe with their own eyes. A complete record of employee performance exists in the printout.

Health and safety issues.

Video data terminals caused by strain, headaches, backaches, stiff backs, and sore wrists.

Repetitive strain injury (RSI) can demonstrate itself in many ways, among those is the painful affliction known as carpal tunnel syndrome. An epidemic of RSI now seems to be sweeping the United States and Europe.