

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.