

Social and Ethical Implications of Computer Use

The society in which we live has been so profoundly affected by computers that historians refer to the present time as the *information age*. This is due to our ability to store and manipulate large amounts of information (data) using computers. As an information society, we must consider both the social and ethical implications of our use of computers. By ethical questions we mean asking what are the morally right and wrong ways to use computers.

Ergonomics is the science that studies safe work environments. Many health-related issues, such as carpal tunnel syndrome and computer vision syndrome (CVS), are related to prolonged computer use.

Power and paper waste are environmental concerns associated with computer use. Suggestions for eliminating these concerns include recycling paper and printer toner cartridges and turning off monitors and printers when not in use.

Employee monitoring is an issue associated with computers in the workplace. It is legal for employers to install software programs that monitor employee computer use. As well, e-mail messages can be read without employee notification.

The invasion of privacy is a serious problem associated with computers. Because computers can store vast amounts of data we must decide what information is proper to store, what is improper, and who should have access to the information. Every time you use a credit card, make a phone call, withdraw money, reserve a flight, or register at school, a computer records the transaction. These records can be used to learn a great deal about you—where you have been, when you were there, and how much money was spent. Should this information be available to everyone?

Identity Theft

Identity theft is a growing crime where personal information is stolen electronically in order to make fraudulent purchases or loans.

Computers are also used to store information about your credit rating, which determines your ability to borrow money. If you want to buy a car and finance it at a bank, the bank first checks your credit records on a computer to determine if you have a good credit rating. If you purchase the car and then apply for automobile insurance, another computer will check to determine if you have traffic violations. How do you know if the information being used is accurate? The laws listed below have been passed to help ensure that the right to privacy is not infringed by the improper use of data stored in computer files:

- The **Fair Credit Reporting Act of 1970** gives individuals the right to see information collected about them for use by credit, insurance, and employment agencies. If a person is denied credit they are allowed to see the files used to make the credit determination. If any of the information is incorrect, the person has the right to have it changed. The act also restricts who may access credit files to only those with a court order or the written permission of the individual whose credit is being checked.
- The **Privacy Act of 1974** restricts the way in which personal data can be used by federal agencies. Individuals must be permitted access to information stored about them and may

correct any information that is incorrect. Agencies must insure both the security and confidentiality of any sensitive information. Although this law applies only to federal agencies, many states have adopted similar laws.

- The **Financial Privacy Act of 1978** requires that a government authority have a subpoena, summons, or search warrant to access an individual's financial records. When such records are released, the financial institution must notify the individual of who has had access to them.

The Ethical Responsibilities of an IT Professional

An *IT* (information technology) professional has responsibilities that relate to system reliability. System reliability involves installing and updating appropriate software, keeping hardware working and up-to-date, and maintaining databases and other forms of data. Governments, schools, and employers rely on IT professionals to maintain their computer systems.

In addition to ensuring system reliability, an IT professional must take responsibility for the ethical aspects of the career choice. For example, IT professionals involved in creating software must ensure, as best he or she can, the reliability of the computer software. This means the ethical responsibility of the IT professional includes using the appropriate tools and methods to test and evaluate programs before distribution. A special cause for concern is the increased use of computers to control potentially dangerous devices such as aircraft, nuclear reactors, or sensitive medical equipment.

IT professionals must also consider the impact they have on computer users. Web users for example often rely on data from websites providing real-time information. The information displayed is determined with a program written using a language that accesses a database. The IT professionals involved in such a project have the ethical responsibility to possibly millions of individuals for ensuring, as best they can, accurate data retrieval.

As capable as computers have proven to be, we must be cautious when allowing them to replace human beings in areas where judgment is crucial. As intelligent beings, we can often detect that something out of the ordinary has occurred which has not been previously anticipated and then take appropriate actions. Computers will only do what they have been programmed to do, even if it is to perform a dangerous act.