PRIVACY ISSUES IN THE DESIGN AND USE OF COMPUTERS

Rein Turn
California State University
Northridge, CA, USA

ABSTRACT

In a generic sense, privacy is the freedom from unwanted intrusion or surveillance. In computer applications, privacy issues arise when personal information is collected, stored, processed, disseminated, and used to make decisions about individuals. Privacy is not a technical concept, but both its violation and protection may involve technical means. This paper examines the basic concepts, issues, and technical requirements involved in privacy protection in national and international contexts. Then it analyzes the impacts on privacy protection of new advances and applications of computer technology. It concludes with a discussion of college-level courses on societal impacts of computers, and the subject material that should be included, especially the ethical issues in computing.

1. PRIVACY PROTECTION ISSUES IN COMPUTING

In 1984, the George Orwell's year, it is appropriate to briefly view the Orwellian information technology and compare it with the actual information technology in 1984. In Orwell's vision [1], in store for mankind in 1984 was a totalitarian regime which demanded total loyalty from its subjects. This was to be assured by total surveillance of the subjects, and by manipulating information, past and present. The purpose of the latter was to assure that the rulers were "always right". If their predictions in the past failed to come true, those predictions were changed. Thus books, newspapers, photos, audio tapes, all were "rectified" to match the past to the present, using "speakwrite" devices for rewriting. Surveillance was based on the use of "telescreens", thought police, and complete personal information dossiers on every person. Disloyal individuals were eliminated and all information about them was destroyed -- they were "vaporized".

As we know, Orwell's visions for 1984 have not materialized in England, the scene of his book, or elsewhere [2]. Likewise, telescreens and speakwrite machines have not been developed. However, while the technology for compiling dossiers is in good shape, rectification of history and vaporizing individuals are beyond the state of the art. The real information technology in 1984 is based on computers and their applications: networks of computers, personal computers, remotely accessible information systems, microcomputers embedded in other systems as controllers, and multimedia systems. They support electronic funds transfer systems (EFTS), electronic mail (EM), office automation (OA), artificial intelligence applications, and others. While these are not the tools of a Big Brother, they may have certain undesireable impacts on individuals and on the society.

Among the societal issues in computing are the following, some of which will be discussed later in this paper: individuals' access to information, automation of the work place, computer-aided crime, computer literacy, dependence on computing by individuals as well as the society, ethics and accountability of computer professionals, privacy protection, data security, data flows across national borders, and the impact of computerization on societal resiliency and vulnerability. References [3-13] provide background information on these issues. Privacy protection, transborder data flows, and technical requirements they place on system design are discussed in greater detail below.

Privacy Protection

The foundations for privacy protection stem from documents such as the Magana Carta of 1215 which established property rights in England, and the Fourth Amendment of the U.S. Constitution (1791) which established "...the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures". Subsequently, in 1890, U.S. jurists Warren and Brandeis, wrote [14] that "... [media] have invaded the sacred precincts of private and domestic life... the law must afford some remedy for the invasion of privacy", and laid the foundations of privacy violation as a tort in th U.S. legal theory. Finally, pointing out that even a benign and compassionate government may be a threat, Justice Brandeis wrote in 1928 [15] that "Experience should teach us to be most on our guard to protect liberty when the government`s purposes are beneficial..."

Individual privacy can be invaded in many ways: physical surveillance, eavesdropping, unwanted solicitations, use of personality tests and polygraphs. These collect information about individuals to be stored and used to make decisions about them. Thus, protecting information privacy of an individual becomes an issue. The following are two definitions of information privacy:

- o "Right of individuals to determine the extent that personal information about themselves is given to others" [16]
- o Rights of individuals regarding collection, storage, circulation, and use of personal information about themselves. [9]

The second will be used as the working definition in this paper. In Europe, "data protection" is used in lieu of "privacy". It has been defined as:

- o "The protection of rights, freedoms and essential interests of persons vis-a-vis the processing of personal information relating to them, particularly when computers aid in the processing." [17]

While personal information privacy protection problems arise in manual record-keeping system too, automation of record keeping has made qualitative as well as quantitative changes. Computer technology makes it economical to store and process large volumes of data, permits complex correlations at high speed, allows high-speed access from distant locations and, thus, makes technically feasible for physically decentralized systems to become centralized "logically". This lays the groundwork for integration of data records and assembly of personal information dossiers on individuals. And this is viewed by the public as a threat to their liberties.

There are other problems, too. Since information in computers is not directly readable by humans, they can't determine without the services of the record keeper what information about them is stored. Furthermore, in computer, undetected hardware and software errors can cause information distortions, and information/data can be altered without detection by accident or deliberately. In general, the following privacy-related issues can be identified in record-keeping systems: Proliferation of systems and records, collection practices, data quality, confidentiality and security, universal identifier, data linkages, and automation of decision-making.

Privacy Protection Principles

Privacy protection is a societal policy and value which must be balanced with other policies and values. It is clear that record-keeping on individuals is necessary when privileges are granted (such as the driver's license) or qualification for some benefits is determined. In these cases, the individual foregoes some of his privacy in order to receive the privilege or benefit. This is in the best interest of the society. On the other hand, the rights of the individual must also be considered. To balance these conflicting goals, the society in its record-keeping activities should [18]:

- o Minimize intrusiveness -- balance information collection with benefits to individuals.
- o Maximize openness in record keeping, and data subjects' access to information about them.
- o Maximize fairness in using personal information for making decisions about individuals.
- o Reduce the "power gap" between individuals and the record keepers and users.
- o Create a legally enforceable expectation of confidentiality of personal information and accountability of record keepers.
- o Provide for data subjects ' participation in formulating record-keeping policies.

The principles for privacy protection have evolved over the last decade, beginning with several national studies, advancing with national privacy or data protection legislation, and coming to the current form in the OECD Guidelines [19]. The Code of Fair Information Practices formulated by a U.S. Government advisory committee on privacy [20] was a starting point for these principles:

- o Openness -- the absence of secret record-keeping systems, practices, or use.

- Individual access -- the right of individuals to know what data are kept about them, and how they are used.
- Individual participation -- the right to correct or ammend erroneous records.
- Collection limitation -- restrictions on data that may be collected, and on methods used.
- Use limitation -- restrictions on the use of data for unannounced purposes.
- Disclosure limitation -- restrictions on external circulation of personal data.
- Information management -- requirements to maintain data quality and security.
- Accountability -- clearly fixed responsibility for compliance with privacy requirements.

Developments in Privacy Protection

The developments in privacy protection from the time it surfaced in mid-1960s in the United States, and soon after in Sweden, are listed below in chronological order. The Younger report [21], the Swedish privacy protection study [22], and Westin's databank study [16], all published in 1972, launched the developments listed below:

- U.S.: "Invasions of Privacy" and "National Data Bank" hearings (1960s).
- U.S.: Fair Credit Reporting Act (1969).
- U.K.: Younger Report (1972).
- Sweden: Data Act (1973).
- U.S.: Code of Fair Information Practices (1973).
- OECD: Seminar on Data Protection and Privacy (1974).
- U.S.: Privacy Act of 1974.
- France: Rapport, Commission Informatique et Libertes (1975).
- U.S.: Privacy Protection Study Commission Report (1977).
- Europe: Data protection and privacy laws (1978-80).
- OECD: Guidelines on privacy protection (1980).
- Council of Europe: Convention on privacy and data protection (1981).

Privacy protection efforts in the United States have developed along three lines: the federal government, state and local governments, and the private sector. Federal-level privacy laws apply to the federal government agencies, but with law enforcement and intelligence communities exempted. They also apply to the private sector in financial credit reporting, to educational institutions that receive federal support, and to government access to individuals' banking transaction records.

The states in the U.S. have enacted numerous privacy protection laws [23]. They cover state and local government agencies and also some private sector business areas. Most of the state privacy laws address one or more of the following: employment records, financial credit reporting, insurance and medical records, law enforcement and criminal justice records, EFTS and cable television, the use of polygraphs, and the like. While in general it is not likely that new federal-level privacy protection laws will be enacted soon, states are likely to be more active. Thus, the private sector record-keeping systems will remain unregulated on the federal scale, despite the Privacy Protection Study Commission's recommendations [18]. In the states, however, regulation of private sector record keeping is more likely.

The perception of the U.S. public is, however, that privacy violations are likely to increase. The 1983 Harris poll [24] shows substantial concerns over possible detrimental impacts of computerized record-keeping on individual freedom:

Opinion on:	Possible	Likely
Disclosure of damaging facts	86%	70%
Use of personal records to intimidate individuals	86	70
Use of closed circuit TV to monitor people	84	67
Use of confidential information to take privacy and liberty	79	58
Use of computer information surveillance to establish a totalitarian regime	63	37

Transborder Data Flows

Many data communication networks, public and private, are international in scope. Multinational corporations with operating units in several countries require business data communication between operating units and the home office, and between the operating units themselves. In other applications, service bureaux and information systems are available to customers around the globe. Data transmissions in these systems are called "transborder data flows". The operators of transnational computer networks tend to be in a few industrially developed countries (such as the United States). Organizations in many other countries are their clients. Typically, the latter are not pleased with being subscribers to, rather than providers of computer services. They would like self-sufficiency in computing, retain the data processing revenues, and generate employment in data processing. When personal data are involved, they fear loss of privacy protection as the data are sent to countries which may have less privacy protection than the home county. Countries that provide international data services or operate private networks tend to view these concerns as without merit and, instead, promote the principle of "free flow of information".

Since the United States is one of data processing service providers, it may be of interest to compare privacy protection laws in the United States with those enacted in European countries. In data subjects covered, an innovation in Europe (especially in Austrian, Norwegain and Danish data protection laws) has been the inclusion of "legal persons" in the set of protected subjects. No such provision is in any privacy law in the United States, nor is it likely to be enacted.

Another major difference is in systems covered -- both private and public sectors in European laws, but only limited private sector activities in the U.S. Finally, enforcement is "corrective" and based on self-enforcment or court actions in the United States, while it tends to be "preventive" and enforced by special government bodies in Europe. These differences are viewed as making privacy protection in the United States weaker than in Europe, and justifying constraints in data flows to the United States. On the other hand, there is in the United States a much stronger tradition of protecting individual rights and freedoms than in most of the European countries. Standardization of privacy protection, such as acceptance and implementation of the OECD privacy protection guidelines, is one response of the U.S. private sector community to the potential threat of constrained transborder data flows. The views of many governments on the TDF issues is reflected in a survey commissioned by OECD [25].

TDF issue:	Percent (Yes-?-No)	
	Total	Western Europe
Free flow of information	39-39-22	50-49-01
National sovereignty	60-38-02	62-38-00
Procedures for access and data exchange	52-46-03	37-68-00
Equivalent privacy protection	61-32-07	87-13-00
Reduction of dependency on foreign DP	45-52-03	25-62-13

Technical implications of Privacy Protection

The technical impact of privacy protection requirements is the incorporation into a personal information record-keeping system's design and operating procedures a number of functions not normally needed [26]. These include: (a) preparing official notifications of the system's functions and procedures in using personal information, (b) facilities and procedures for inspections, challenges, reviews, and submitting corrections or rebuttals by individuals, (c) accounting for, and auditing the collection, use, and disclosure of personal information, and interactions with the data subjects, (d) achieving and maintaining data quality, (e) maintaining data confidentiality and security, and (f) demonstrating compliance with privacy protection requirements.

Collectively, these technical requirements imply more computational tasks to be performed, and more data storage resources to be used. For example, the Privacy Act of 1974 requires that "...agencies shall maintain all records with such acuracy, relevance, timeliness, and completeness as is reasonably required to assure fairness to individuals in determinations".

This calls for the following policy decisions to determine: data items to be used (relevance), the level of detail of information items (precision), the retention time (timeliness), and criteria for verifying accuracy of factual and evaluative information. In addition, mechanisms must be provided for assuring authenticity of the data items, for access authorization, and for revalidation or purging of data items.

These, in turn, call for error control in data collection and entry, reliable identification of individuals, maintaining data integrity in the system, providing additional data fields in records for privacy information, providing privacy protection related audit trails, implementing in the systems data security safeguards and acces control mechanisms, and adequate provisions for system backup and recovery.

Data security requirements in national data protection laws, and in international agreements, provide another example. The Council of Europe convention [27] provides that: Appropriate security measures shall be taken " ... against accidental or unauthorized destruction or accidental loss, as well as against unauthorized access, alteration or dissemination". In addition, the convention requires that specific security measures be provided for every file; that the degree of vulnerability, need to restrict access, and requirement for long-term storage be considered; and that the current state-of-the-art security measures, methods, techniques be used.

Concluding this section, it may be observed that privacy protection continues as a concern in industrialized countries, and that privacy protection principles are well-formulated and implementable. In the United States, federal-level privacy protection legislation is stalled, but the state level legislation moves on. In Europe, several countries are moving toward enacting data protection legislation [29]. Since the technical aspects of privacy protection requirements are substantial, they must be considered early in the system's design phase and maintained throughout its lifecycle.

2. PRIVACY IMPACTS OF NEW TECHNOLOGIES

Computer technology advances in the last decade have resulted in making available, at acceptable cost, virtually unlimited processing power, storage capacity, and data communication capabilities. The very large scale integration (VLSI) technology permits placing on a chip tens of thousands of logic circuits and millions of bits of memory, and to mass-produce these for near-negligible cost. It will be economical, therefore to maximize the use of computer technology in any system. Such use produces old products and services in new, digital form, and engenders new services. Digital telephone, digital transponders, and cellular radio are examples from communications area.

In other application areas, a microprocessor and memory can be embedded in a plastic card to produce the "smart card" now being tested extensively in France. Signal-processing using special-purpose processors can be coupled with digital video scanners to analyze visual scenes for specified objects, even human faces. Speech recognition is advancing, and progress is being made in analyzing human bio-variables to monitor body functions, and mental or emotional conditions. Extensive research is underway in the so-called fifth-generation systems to augment computational capabilities with knowledge storage and processing [30,31].

There are several applications of the new computer technology which must be analyzed from the point of view of societal impacts. A new applications will always have beneficial effects which will justify its development, but it may also have potentially detrimental impacts. The latter are usually not explored or they are "swept under the rug". In this paper, the focus is on potential threats of new applications to personal information privacy and to other individual rights.

Applications such as computer networks, electronic mail, EFTS, smart cards, interactive home services, and embedded microprocessors tend to have a set of common attributes or modes of operations which increase their potential for adverse impacts on privacy protection as they potentially support:

- o Vast, integrated, personal information record-keeping systems.
- o Automated services that generate large volumes of transactions involving individuals, and keep records on these.
- o Automated techniques and systems for collecting and transmitting computer readable personal information.
- o Applications and services that allow inferring personal information.
- o Direct or indirect integration of systems which handle personal information.
- o Automation of decision-making based on personal information about individuals.
- o Physical or informational surveillance of individuals.
- o Overt or covert commercial markets for personal information.

The above features of many new applications of computer technology set the stage for potential privacy protection problems. For example, connecting computers into networks, and networks into super-networks, is progressing rapidly. The benefits for data communication are obvious. However,the resulting systems contain multitudes of complex, hard-to-trace communication paths which contribute to problems in providing security, access control, and message intrgrity and authenticity.

From privacy protection point of view computer networks where personal information data bases are on-line can support de facto integration of record-keeping systems and, thus, the capability for "virtual dossiers" and extralegal exchanges of personal information. Networking will also enhance matching of personal information files in different systems for investigative purposes [32,33], increase the difficulty in monitoring compliance with privacy protection requirements, and render more difficult the detection of attempts to misuse personal data bases. For example, setting up commercial databases of sensitive personal information culled from networked systems, or disclosing personal information in public bulletin boards. These seem to exist openly or clandestinely in all networks.

Similar privacy protection problems arise in other new applications. Electronic mail is being developed to replace the traditional postal letter delivery services by facsimile or digital text. The possible privacy protection impacts are: misuses of mail transaction files, covert interception and copying, surveillance via key-word scanning of digital messages, electronic "mail covers", illicit search of "electronic mailboxes", and covert disclosure or sale of electronic mail transaction information.

Privacy problems of electronic funds transfer systems have been analyzed extensively [34,35]. They include: (a) collection of large amounts personal information, (b) inference of additional personal information from EFTS transaction files, (c) capability for information-based surveillance of individuals and generation of dossiers, using EFTS files for making decisions about individuals which are not related to EFTS, (d) disclosures of EFTS transaction information commercially or to the authorities, and (e) inability to prevent unauthorized access, modification, or disclosure of personal information in EFTS transaction data bases.

Smart cards can be used as record carriers for many applications. If personal information is stored on the card, privacy protection problems arise. Now the card becomes a portable file system, and it can be the link that integrates different personal information systems. The privacy protection concerns for individuals involve the ability to exercise existing privacy rights. In particular, to know precisely what information is being stored on the card, how is it used, and what prevents unauthorized access to information on the card in situations where more than one service is provided with the same card. Similar problems arise regarding data security on the card.

Interactive home services are usually based on the use of two-way cable service connected to the home television set and a primitive terminal. Services provided include home banking, purchases, access to information data bases, interactive entertainment, public polls, and the like. Privacy protection problems arise due to:

- o Large files of personal transaction data.
- o Possibility for generating dossiers of personal or household information.
- o Data misuse for other purposes, overtly or covertly; data sales or theft.
- o Forced disclosure to legal authorities.
- o Lack of legal support for exercising privacy rights.

Personal computers are now in millions of homes. They have become powerful systems with vast capacity for off-line storage of computer readable data, and with large selection of sophisticated, low-cost software. They are easy to connect into data communication networks, and are readily usable by almost anybody. However, a personal computer at home or office can also used to invade other persons' privacy, to circumvent privacy protection requirements, and to attempt unauthorized access to personal information record-keeping systems or other systems.

Personal computers or workstations are the foundation of office automation which is now sweeping through industrialized countries. The services provided include word processing, data base management, program development, applications program execution, a variety of transactions, and electronic mail. Connection to mainframe computer systems, and to public or private networks is growing, as is dial-up access. Potential problems are in access control and security [36], monitoring of employee work and productivity, inspecting personal files, and generation of personal information dossiers on employees. A new consideration is that employees themselves may become privacy violators, on their own or as directed by the management. This may set the stage for civil legal actions by the victims on the grounds of defamation of character or libel.

The massive availability of low-cost microprocessors and read-only memories has accelerated their use as controllers, instrumentation, or information collectors in many systems: automobiles, appliances, home systems (security, energy use control), business security, law enforcement, etc. Some provide for remote readout over wire, or use digital transponders. Their use can generate extensive data bases, on system's premises or at remote locations. From these, information may be inferred about personal activities of individuals, in real time or as behavior profiles generated after the fact. Likewise, an individual's location can be determined and his movements monitored by a remote readout transponder in the automobile, such as the "electronic license plate". There are also potentials for covert information collection for surveillance, and unauthorized interception and file compilation. There are difficulties in enforcing privacy protection requirements and individual`s privacy rights.

Artificial intelligence is a field in computer science which is now developing rapidly. The fifth generation computer architecture research efforts in several countries are focusing on applications such as knowledge data bases and inference generation. Other applications are natural language understanding, speech understanding, visual pattern and scene recognition, and expert systems for decision support. However, these applications also have a potential for enhancing surveillance techniques, automated real-time tracking of individuals, generating psychological profiles, and intimidation and manipulation of people.

Since the technology applications examined above have significant benefits, their development should not be hindered. Rather, means must be found to lessen the potentially adverse impacts on individual privacy and freedoms. Among the available approaches are the following:

- Legislation to strengthen privacy protection, and extend it to new applications.
- Technical measures to protect against unauthorized actions.
- Reliability and integrity measures to prevent accidental privacy abuse.
- Personnel techniques to create and maintain privacy awareness.
- "Watchdog" groups of computer science professionals and "lay" citizens to monitor new system developments.
- Sensitizing computer science students to potential misuses of computers.

The above remedies can lessen, but not entirely eradicate the privacy protection problem. New computer applications will be developed despite the clear potential for violating personal privacy and freedoms -- the technological imperative is at work. Thus, it is important that the developers and operators of new computer technology applications be made aware of the problem, and induced to take corrective action. In particular, legislative measures must be enacted to provide privacy protection. Finally, computer professionals must become and remain societally responsible and vigilant.

3. COURSES ON SOCIETAL IMPACTS OF COMPUTERS

It is abundantly clear that computerization of industrial societies is accelerating at an increasing pace. Computer applications are seen to be the way out of economic problems and sagging productivity [5]. Less developed countries see in computers and access to data bases a magic solution to their development problems. At the 1978 world congress on Strategies and Policies on Informatics (SPIN) [36], it was stated that "information [and informatics] is more than a form of power, it is an entire power system itself: it allows countries and people to make use of other technologies".

Computer applications are indeed generating great societal benefits and economic progress. However, with the broadening of the scope of their use, computer applications may also endanger human life or health, and be detrimental to individuals or the society. Thus, it is likely that, in the future, society will demand full accountability of computer applications developers and users. It is becoming increasingly important for the computer professionals to be able to analyze societal impacts of proposed applications and to know how to minimize the potential harms. This, and other aspects of computer use, raise important ethical and legal questions which computer professionals must understand. One approach to conduct educational programs aimed at practicing professionals and, in particular, at the students in computer science.

Computer and Society Courses

"Computers and Society" courses are often found in colleges and universities as entry level computer literacy courses. Often they mention societal issues only in passing, and devote most of the time teaching programming in BASIC. This is not adequate for teaching computer science students professionalism and ethics, and sensitizing then to the growing societal concerns about computers and their applications. A serious course on societal impacts requires students who are already mature in computer technology and, thus, should be offered to students close to completion of the curricular requirements. The course objectives should be to:

- Sensitize students to societal issues and impacts: benefits vs. drawbacks.
- Survey the history and development of the computer field.
- Examine societal issues in several computer applications.
- Discuss good practice as well as pitfalls in computing.
- Examine the professional aspects of practicing in the computing field.
- Teach about ethics and legal requirements or responsibilities.
- Develop communication skills -- both oral and written.

Several computers and society course have ben described in literature [37], and the results of an ACM project on such courses, and on computer literacy questions in general, has been published [38].

A Computer Impacts on Society Course at CSUN

One such course has been offered at the California State University, Northridge, every smester since 1978. It is a required course in the computer science core at the senior (fourth year) level. It is a lecture/discussion course of 45 class hours, limited to a maximum of 35 students. The requirements of the course include preparation of a term research report, two midterm tests, the final exam, numerous reading assignments, and participation in class discussions. Oral presentations of term reports is optional. Over the years, several text have been used, with a compendium of essays on computing edited by Dertouzos and Moses, "The Computer Age, A Twenty-Five Year View", MIT Press, 1979, the current required text. As a rule, seniors at CSUN are quite mature in computer science, and many have work experience in computing. An abbreviated outline of the course material is as follows:

- Societal concerns and issues.
- Technology assessment.
- Historical developments in computing.
- Advances in computer technology.
- Technology assessments of selected applications: MIS, use of models, EFTS, OA, EM, CAI, CAD/CAM, AI.
- Privacy and security issues.
- Professionalism in computing.
- Codes of ethics, ethical issues.
- Legal questions in computing.

The societal issues discussed in the course have already been examined earlier in this paper. In general, they deal with problems in automation and employment, benefits of computer use, computer-aided crime and fraud, computer literacy, dependence on computational models, ethics and accountability, privacy protection, computer and data security, societal resiliency or vulnerability due to computerization, and transborder data flows. The approach used is based on the technology assessment methodology [39]. This involves, briefly, the following steps:

- Define the assessment task and scope.
- Describe relevant technologies.
- Identify nontechnical factors.
- Develop state-of-society description.
- Identify societal impact areas.
- Perform impact analysis.
- Identify action options to minimize undesireable consequences.
- Make the final assessment.

Examples of the impact areas to be considered include: value systems (individual, group, national), individual rights and freedoms, environmental problems (pollution), demographic considerations (migration, density), economic aspects (employment, productivity), social issues (health, education, welfare), and institutional imapscts (political, legal). The purpose is to identify the problems, and recommend corrective actions. Examples of the latter are: control over funding, tax policies, legislation and regulation, licensing and reporting requirements, publicity in media, education and explanation, studies and research, and political actions.

Ethical Problems in Computing

Teaching about ethics and good practice in computing poses special problems because of a lack of materials. In the United States, there is no widely accepted Code of Ethics for the computing profession, although ACM and other organizations have published their own [39,40]. In England, the situation is better due to the British Computer Society's "Code of Good Practice". An excellent source on material on ethics is a relatively recent AFIPS study [41]. Below are examples of ethical issues which should be examined:

- Hacking, attempting to gain unauthorized to computer systems or files.
- Browsing in others users' computer files.
- Making unauthorized changes in programs or data bases.
- Attempting to avoid charges for computing or communication.
- Inviting users to "crack" computer security safeguards.
- Revealing information on accessing the employer's computer or files (e.g., submitting to bulletin boards).
- Using employer's computing resources for for personal business.
- Marketing employer's programs or data without permission.
- Copying employer's programs for own use.
- Copying copyrighted programs for own or friends' use.
- Taking programs written with employer's resources when leaving.
- Sabotaging competitors' efforts, for own or employer's benefit.
- Attempting to evade responsibility or accountability for mistakes or bad judgement.
- Claiming expertise beyond actual knowledge or experience.
- Designing systems with potentially harmful societal impacts.
- Failing to alert management of potential societal harms of a development.
- Attempting to market or claim as complete a deficient piece of work.
- Using others' work without permission or giving credit.

- o Writing programs or using data to produce deliberately biased results.

It must be pointed out that the above are only statements of ethical issues. Whether or not the item turns out to be unethical or not unethical may depend on the circumstances. It certainly depends on subjective judgements, as illustrated in the considerable range of disagreement over the scenarios discussed in [41]. One of the ethical issues currently in the public spotlight is hacking [42,43]. Involved are bright young people who are experts in the use of some computer system, and who seem to be obsessed with computing. They seem to believe that they are intellectually superior, and they seem to claim an intrinsic right to access any system of their choice. They are encouraged by media coverage, movies, and television shows where they are depicted as heroes, rather than as villians. They have even been praised by some computer scientists [42].

Hackers typically choose a target or stumble on one by trial and error search for dial-up access numbers. They may obtain access codes and passwords from bulletin boards in computer networks, may use default passwords left in the system, or attempt trial and error searches. If they succeed, they may plant "hooks" in the system for future entries, browse around, leave messages, and damage data or programs. Victims must spend resources to undo the damage and strengthen the protective system. All of the above, and more, were involved in the exploits in the U.S., of the so-called "414 group" [43]. Neverheless, they were called "information age Robin Hoods" by media, and were thanked for doing "a service to the country" by a U.S. Congressman. Clearly, hacking is a perplexing ethical problem to many.

There are numerous technical measures that can be taken to curb hacking, such as the use of dial-up access control units [44]. The ethical dilemma may be solved, however, by legislation. New computer-crime laws in the United states have defined any unauthorized access to computeer systems a misdemeanor offense or trespass, and federal legislation is expected to take the same position. More generally, steps are being taken to promote security awareness of employees and users, and to sensitize to ethical aspects of hacking and computing in general. Computer impacts on society courses are a part of this program. One step that can be done immediately is to add a warning statement to the computer log-on page, such as: "If you have not been authorized to access this system, you are trespassing and subject to prosecution under section [X] of the criminal code [Y]. Do not proceed to enter the system."

In conclusion, "Societal Impacts of Computing" should be a required course in any computer science curriculum, taken just before graduation. Emphasis should be on the societal issues and impacts of computing, methods to analyze societal impacts, ethics, codes of conduct and good practices, the legal requirements which may apply, and on becoming and being a professional in the computing field. Such a course should be the capstone of education in computing and a gateway for students to enter the profession with a sense of responsibility and accountability to the society.

REFERENCES

1. Orwell, George, "1984", The New American Library, Inc., New York, 1964.
2. "Georege Orwell", The Futurist, January 1984.
3. "Computer-Based National Information Systems", Office of Technology Assessment, U.S. Congress, Washington, DC, September 1981.
4. Mumford, E., and H. Sackman, "Human Choice and Computers", North-Holland Publishing Co., Amsterdam, 1975.
5. Nora, S., and A. Minc, "The Computerization of Society", MIT Press, Cambridge, MA, 1980.
6. Parker, D.B., "Fighting Computer Crime", Charles Scribner Sons, New York, 1983.
7. Norman, A.R.D., "Computer Insecurity", Chapman and Hall, London, 1983.
8. Westin, A., "Privacy and Freedom", Atheneum Press, New York, 1967.
9. Turn, R., "Privacy Protection in Information Systems", in Advances in Computers, Volume 16, Academic Press, New York, 1977, pp. 221-335.
10. Hondius, F. W., "Emerging Data Protection in Europe", North-Holland Publishing Co., Amsterdam, 1975.
11. "Transborder Data Flows and the Protection of Privacy", ICCP-1, OECD, Paris, 1979.
12. Turn, T. (Ed.), "Transborder Data Flows: Concerns in Privacy Protection and Free Flow of Information", AFIPS Press, Reston, VA, 1979.
13. Turn, R. (Ed.), "Observations on the Resiliency of the U.S. Information Society", AFIPS Press, Reston, VA, November 1982.
14. Warren, S., and L.D. Brandeis, "The Right of Privacy", Harvard Law Review, Vol. 4, 1890, p. 193+.
15. Brandeis, L.D., in Olmstead vs. Uniteed States, U.S. Supreme Court decision, 1928.
16. Westin, A. F., and M.A. Baker, "Databanks in a Free Socity: Computers, Record-Keeping and Privacy", Quadrangle Books, New York, 1972.
17. Hondius, F. W., "Data Law in Europe", Stanford Journal of International Law, Volume 16, Summer 1980, pp. 87-111.
18. "Personal Privacy in an Information Society -- The Report of the U.S. Privacy Protection Study Commission", U.S. Government Printing Office, Washington, DC, July 1977.
19. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", OECD, Paris, 1981.
20. "Records, Computers, and the Rights of Citizens", U.S. Government Printing Office, Washington, DC, July 1973.
21. "Report of the Committee on Privacy", K. Younger (Chairman), H.M. Stationery Office, London, July 1972.
22. "Data och Integritet", Report of the Royal Committee on Publicity and Secrecy, Stockholm, 1972.
23. "Compilation of State and Federal Privacy Laws, 1984-85 Edition", Privacy Journal Publishing, Washington, DC, 1984.
24. "The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy", Sentry Insurance Co., Stevens Point, WI, 1983.
25. "Survey of World Opinion on TDF", TDR Report, 1982.
26. Turn, R. (Ed.), "Technological Implications of Privacy Protection", IEEE Computer Society, July 1979.
27. "Convention on Protection of Individuals with Regard to Automatic Processing of Personal Data", Council of Europe, Strassburg, 1981.
28. Data Commissioners Review International Problems", TDR Report, December 1983.

30. Mota-Oka, T., (Ed.), "Fifth Generation Computer Systems", Nortrh-Holland Publishing Co., Amsterdam, 1982.

31. Hertzberger, L.O., "The Architecture of Fifth Generation Inference Computers", Future Generation Computer Systems (North Holland Publishing Co, Amsterdam), Vol. 1, No. 1, July 1984, pp. 19-21.

32. Shattuck, J., "Computer Matching Is Serious Threat to Individual Rights", Communications of the ACM, June 1984, pp. 538-541.

33. Kusserow, R.P., "The Government Needs Computer Matching to Root Out Waste and Fraud", Communications of the ACM, June 1984, pp. 542-545.

34. Benton, J.B., "Electronic Funds Transfers: Pitfalls and Payoffs", Harvard Business Review, July-August 1977, pp. 16-32.

35. Kling, R., "Electronic Funds Transfer Systems and Quality of Life", Proceedings, 1978 National Computer Conference, AFIPS Press, Reston Va, 1978, pp. 191-197.

36. "Strategies and Policies on Informatics", Documents from SPIN Conference, Unipub, Newe York, 1978.

37. "Special issue: Computers and Society Courses", Computers & Society (ACM), Vol. 12, No. 4, Fall 1982.

38. "Project: .Computer Impact on Society and Computer Literacy Courses and Materials", Computers & Society (ACM), Vol. 11, No. 3, Summer 1981

39. Jones, M.V., "A Technology Assessment Methodology", MTR 6009, The Mitre Corporaion, McLean, Va, June 1971.

40. "ACM Code of Professional Conduct", Communications of the ACM, March 1982, pp. 183-184.

41. Parker, D.B. (Ed.), "Ethical Conflicts in Computer Science and Technology", AFIPS Press, Reston, VA, 1981.

42. "Computer Capers", Newsweek, September 5, 1983, pp. 42-48.

43. "Computer and Communications Security and Privacy", Hearings, U.S. Congress House Committee on Science and Technology, September/October 1983, U.S. Government Printing Office, Washington, DC, 1984.

DISCUSSION

Lecture 1

There was some light hearted discussion on privacy and security issues concerning satellite T.V. In the same vein Professor Whitfield observed that wearing of spectacles is strictly speaking illegal in the U.K. since their owners receive and transmit electromagnetic signals and yet do not possess a licence!

Lecture 2

Professor Randell inquired whether existing legislation was sufficient. Professor Turn replied that in the U.S.A. the existing legislation was inadequate. There is no legislation which covers the private sector which is where the worst of the activities mentioned take place, though the public sector is at least partially covered.

Mr. Davies asked whether Professor Turn thought that there should be a right to privacy in correspondence. Professor Turn replied that there should certainly be a right to privacy, and stated that there is a legal right to confidentiality within first class mail sent in the U.S.A.

Mr. Davies agreed but thought that problems may occur when trying to preserve privacy across national boundaries. Professor Turn agreed but mentioned the opposite point of view where a country should have a right to see what crosses its borders. Mr. Davies pointed out that CCITT recommendations state countries have a right to look at correspondence only in relation to security matters if it is thought that national security may be breeched.

Lecture 3

Noting the fact that Professor Turn's course is given to final year university students, Professor Gilles observed that many high schools in the U.K. teach courses on social impact of computers. Professor Turn thought this to be a good trend since many 'computer hackers' are high school students. Professor Cohen remarked that the course contents had a rather strong technological bias as against philosophical. Professor Turn agreed, saying that the course reflected his own expertise. Finally, Mr. Kenny remarked that the British Computer Society's 'code of good practice' for its members is now known simply as a 'code of practice'!