

# Agenda for the Study and Teaching of Information Technology Ethics

**ABSTRACT:** *The study of ethics in the development and use of information technology is growing. Many universities have included the topic in their curricula either as a module in computer science or information systems courses, or as a separate course fully devoted to the subject. A growing number of researchers study ethical concerns that are involved in the development and use of information systems. This paper provides an agenda for the study and teaching of ethical concerns and dilemmas among which are: privacy, freedom of expression, professional conduct, computer crime, software intellectual property, and obligations of software developers.*

**KEYWORDS:** *Information Technology, Information Systems, IT Professionals, Ethics, Ethics Education.*

## INTRODUCTION

The advent of computers has changed many aspects of our lives. It has eliminated some occupations, changed many people's work environment, altered the methods used by teachers to educate children, rearranged organizational structures, affected the way we shop and the manner in which we use money, and changed the ways in which organizations and individuals communicate. This new technology can make our lives happier, but it may also make us miserable, and it has already promoted new types of crime.

In 1986, Richard Mason discussed the four ethical issues that he considered to be the most important: Privacy, Access, Property, Accessibility (PAPA) [4]. The article provided a good platform for discussion of the issues. Since then, ethical concerns have become more complex. The number of articles and books in the area of computer ethics has

grown. Professional organizations such as the Association for Computing Machinery (ACM) and Data Processing Management Association (DPMA) encourage educators to include the topic in their curricula.

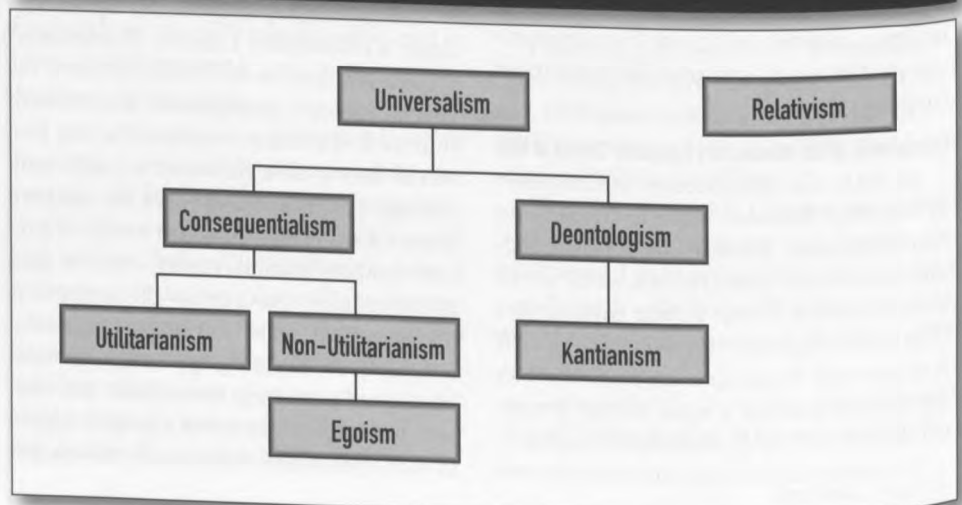
The growing interest and serious concern call for a formulation of an agenda for research and teaching. The purpose of this paper is to outline the issues and propose such an agenda. The general topic of information technology (IT) and ethics is broken down into its components. For each component, the issue is elaborated, and topic for research and teaching are offered.

## ETHICAL THEORIES AND THE EVOLUTION OF ETHICAL CODES

It is difficult, if not impossible, to discuss an ethical issue without referring to an ethical theory. When one makes an argument it should be implicitly or explicitly anchored in some ethical doctrine. Both students and researchers should be aware of the different approaches to the question of why the same act may seem ethical to one person and unethical to another person. Unfortunately, for researchers and students whose main interests lie in the technology, not in the philosophy of morals, navigating the map of ethical thinking may be confusing. Figure 1 presents the main ethical theories and the interrelationships among them. Researchers should conduct their studies, implicitly or explicitly, within the framework of a known ethical theory. Students should be able to evaluate IT development and use with a clear ethical approach to the dilemma at hand. A brief description of widely accepted theories follows.

Relativism holds that an act should be judged in a context; what is unethical in one society may be considered ethical in another

Figure 1: A Map of Major Ethical Theories



society. Therefore, we should not judge other societies by our standards. In the context of IT a relativist could argue, for instance, that government use of computers to track down dissidents in an under-developed country is not unethical because that is "the way of life" in that country. The argument could be made that without this measure there would be chaos in that country.

At the other extreme, universalist theories preach that the same standards should be maintained everywhere by everyone. The main approaches within universalism are the deontologist theories and the consequentialist theories. The deontologist argues that right is right and wrong is wrong regardless of the consequence of the act. It is the intent of the actor that makes the act ethical or unethical. The best known of these theories is Kantianism. We often use Immanuel Kant's categorical imperative "Act only on that maxim through which you can at the same time will that it should become a universal law." Therefore, a Kantianist would argue: "Respect the intellectual property of a software developer because you wish others to respect yours." The Kantianist would not attempt to examine whether this rule increases or decreases the welfare of the public at large or of certain individuals.

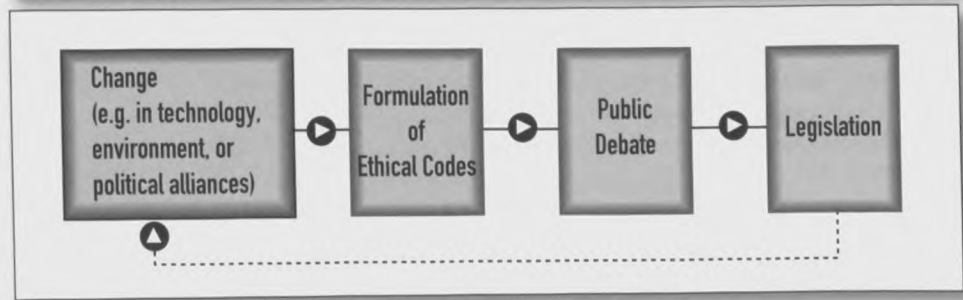
In contrast, consequentialists do examine the results of an act before determining its ethicality. The egoist looks to the consequence, but his rule is: "The act is right because it benefits me," regardless of how the act impacts others. Therefore, egoism is non-utilitarian.

Utilitarian ethicists judge an act by its net result for society. Their motto is: "maximum good for the greatest number." Namely, they try to see if the act results in more good than bad in terms of how much the good outweighs the bad and for how many people. In the context of IT, utilitarians argue that software copyright is unethical because few individuals benefit from it while millions may not be able to enjoy the software because of its prohibitively high price. The Kantian and utilitarian arguments seem to be the most popular in public debates.

When we must decide to forego the good of one party for the good of another party we have an ethical dilemma. IT professionals and other users of information systems should make clear what their approach is when making claims about the ethicality of certain behavior relating to information or information technology.

Initial formulation of ethical codes and public debate will result in appropriate legis-

Figure 2: The Evolution of Ethical Codes



lation. This has been the case whenever a new technology emerged. IT is not an exception.

### "ETHICAL VERSUS LEGAL"

Ethical theories try to provide rationales for answering the question "Is this act ethical?" while "ethical" means "right," and "unethical" means "wrong." Since breaking the law is usually considered wrong, some researchers prefer not to study the ethicality of illegal acts. However, "legal" does not always equal "ethical," and "illegal" does not always mean "unethical."

Law-abiding citizens expect their representatives in legislatures to turn the unethical into illegal in the form of laws. This, indeed, is the purpose of legislation and the mission of legislators. However, few laws have remained unchanged throughout history. Also, many aspects of our professional and private lives would be free of ethical dilemmas if we could count on laws alone to make decisions.

Those of us who conduct research in the intersection of ethics and IT are encumbered with the task of finding what different parties believe to be right or wrong. The parties are the public at large, members of the IT profession, and the clients who consume the services and products of IT professionals.

Educators are obliged to equip their students with the tools that will help them make decisions when in an ethical dilemma. An increasing number of IT educators recognize that they should not settle for providing technical education, but also caution their students about the consequences of unprofessional conduct. Perhaps they should begin by explaining the term ethical in light of the above ethical theories and by delineating the lines between the concepts of "ethical" and "legal."

Table 1 provides examples of four categories of acts: legal and ethical, illegal and unethical, legal but unethical, and ethical but illegal. Of course, some people would say that helping a fugitive is unethical even if you know he is innocent, but this is because to them it is unethical to violate any law, not be-

cause the act is inherently wrong. The point is not to stir ethical arguments, but to advocate that an issue should not stop to be debated just because it is addressed by a law. Laws are changed due to public debate.

Here are two examples in the IT field. Vermont law does not proscribe the launching of a computer virus into private computers. Does that mean the act is ethical in that state? California law authorizes the state to forfeit a computer that was involved in a computer crime. It is legal, but is it ethical?

### TOPICS IN INFORMATION TECHNOLOGY AND ETHICS

In a landmark article, Mason (1986) suggested that there were four issues to be addressed in the information age: Privacy, Accuracy, Property, and Accessibility, acronymed PAPA. The article provided a useful framework for discussion, debate, and research on the topic of IT and ethics. Two of the issues, privacy and accessibility, dealt directly with privacy. The other two, accuracy and property, also, dealt with privacy, albeit indirectly. Property addressed the important question of ownership of information and the media through which information is transferred. (Some of us would use the term "cyberspace" for the media.)

Unfortunately, the article did not deal with other important issues as will be elaborated here. The rise of a new type of crime, collectively termed "computer crime," raises important ethical questions. The emergence of a new profession and the IT professional, invokes questions about the obligations of IT specialists. And the proliferation of software must be addressed with proper codes regarding the intellectual rights of the developers and the obligations of software developers to the users of their creation. In addition, it is important to alert IT students of impending ethical issues that are related to new technologies. Researchers should be aware of the moral implications of such technologies and study the public's preferred ways to deal with them. The following discussion elaborates the issues,

Table 1: The Four Categories of Ethicality and Legality (samples from USA)

<p><b>Ethical and Legal</b></p> <ul style="list-style-type: none"> <li>○ Charity</li> <li>○ Voting</li> </ul>	<p><b>Ethical but Illegal</b></p> <ul style="list-style-type: none"> <li>○ Stealing medication for a person who would die without it and who cannot afford it</li> <li>○ Assisting a fugitive you know is innocent</li> </ul>
<p><b>Legal but Unethical</b></p> <ul style="list-style-type: none"> <li>○ Slavery in U.S. and Brazil until 2nd half of 19th century</li> <li>○ Persecution of Jew in Nazi Germany</li> <li>○ Adultery</li> </ul>	<p><b>Unethical and Illegal</b></p> <ul style="list-style-type: none"> <li>○ Murder</li> <li>○ Theft</li> <li>○ Bribe</li> <li>○ Polygamy</li> </ul>

and suggests teaching techniques and research questions.

## PRIVACY

With all the importance we attach to it, privacy is not even mentioned in the US constitution nor in the constitutions of many other democratic nations. Yet, we consider it one of the most important values in a free society. What is privacy and why is it so important? Privacy is a situation where an individual has control over information regarding himself or herself. Invasion of privacy is the partial or full lack of control over facts relating to our lives. In a society that espouses the individual's right to pursue happiness, invasion of privacy may hinder the individual's effort to achieve a better life.

Our society esteems personal achievement and growth. We look to the individual to endeavor and succeed. Through individual development, society augments its knowledge and raises its standard of living. Privacy is essential for individual growth. It allows a person who erred at a younger age to pursue his or her dreams as an older and wiser person. It guarantees that an embarrassing event in one context of one's life does not compromise his or her quest for excellence in another context. It ensures that prejudice does not limit a sincere effort to leave an old spurned self and evolve into a new accepted self. Thus, privacy allows the delinquent juvenile to become a great scientist, and the unorthodox thinker to establish a new school of thought, and all of us to adapt to new ideas and conventions in a changing society [9].

There are two types of privacy issues: organization-individual, and organization-employee. The first issue is between organization, either government agencies or private organizations, vis-à-vis private people in their capacity as citizens and consumers. The sec-

ond issue is between an organization as an employer and individuals as employees.

### Citizen and Consumer Privacy

The dilemma is how to balance the interest of disparate parties. Three parties are involved in the issue of privacy: government, commercial organizations, and the individual. As a society we must balance the interest of the government versus the rights of the individual; we also must balance the interests of commercial organization with the concerns of the individual. Graphically, we have a seesaw situation, as depicted in Figure 3.

Governments must collect data on individuals for effective tax collection, law enforcement, economic and infrastructure planning, granting voting rights and determining voting zones (e.g., congressional districts), and military draft. All are legitimate needs without which governments cannot function. Therefore, at least vis-à-vis the government, no individual can have absolute privacy. As individuals, we must give up some of our privacy for the services we receive directly as private people, or indirectly, as part of a nation.

Citizens, on the other hand, want assurances that the government collects and maintains only the data needed for the above purposes. In a democracy, the principle should be: let us know as much as possible about the government's affairs; let the government know as little as possible about our private affairs.

Private organizations, too, have much interest in us, as consumers. They collect massive amounts of data that range from addresses to drinking habits. The benefits that individuals receive are in the form of better and cheaper products and services. Access to information democratizes the private sector because both the large, well-established company and the

small fledgeling business have an equal chance at targeting their markets. Again, the dilemma is whose interests to promote, the organization's or the individual's.

### Employee Privacy

Collection of information that does not relate directly to a person's work for an employer constitutes invasion of privacy. Protection of individual privacy should be balanced with legitimate business needs. For example, monitoring an employee's consumption of alcohol at home is an invasion of privacy, but is not if the employee has a known alcohol problem and operates the firm's machinery or a vehicle. Behavior that does not directly affect performance or co-workers should not be monitored. The problem is how to determine, case by case, whether a certain behavior affects productivity of the employee or the employee's peers.

Modern information technology enables employers to effectively monitor their employees. In addition to video cameras and telephone tapping devices, computers are now used to track transaction entries, to intercept electronic mail (E-mail), and to check almost every other activity. Many managers maintain that "people won't do what they are expected to do, but what they're inspected to do". It is estimated that 26 million American workers in more than 60,000 companies are subject to electronic surveillance [5, 11]. Of these employees, 4 million to 6 million are monitored by computers [6]. Among US office workers, probably as many as 50% are monitored [13].

Employers electronically monitor employees for two reasons: productivity and security. Security includes prevention of theft and fraud. Measuring employee output is legitimate. Monitoring to deter theft or sabotage, too, is legitimate. But there is evidence that many employers collect data that are not used for these purposes. The dilemma is how to balance the legitimate needs of the employer with the privacy and dignity of the employee, as illustrated in Figure 4.

### Finding the Modus Vivendi

To balance the rights of the individual on one hand, with the interests of governments and private organizations on the other hand the following principles should be followed by those who collect and maintain personal data: *Purpose.* Determine a specific purpose for collecting and maintaining the data, and ensure that the data object understands how the data will be used. Use the data only for this purpose unless the data object has consented to a different usage. Example: information on psychiatric treatments obtained by an insurance company could put a per-

son in a vulnerable situation if the information is passed on to a political rival or business competitor of that person.

**Relevance.** Record and use only those data necessary to fulfill your purpose. For example, an applicant's credit file should not contain the applicant's political views, because such information should not be used in credit considerations. An example of using irrelevant data would be a denial of a job to an individual who was arrested but has never been convicted.

**Accuracy.** Ensure that the data are accurate. For example, many loan applicants have had terrible experiences due to erroneous data held by credit history companies. Accuracy can be enhanced through careful data entry and periodic verification.

**Currency.** Make sure that all data about an individual is current. If you cannot guarantee currency, it would be fair to discard the data altogether. Data that were correct a while ago may no longer be correct now. For example, a person might have been in a physical condition that would prevent him from being hired for certain positions. That person may be healthy now. If his record does not reflect the change, he may be denied employment.

**Security.** Limit access to the data to only those who need to know it. Security includes the physical limitation of access to computers and terminals, the use of access codes and passwords, and the establishment of audit trails.

**Time Limitation.** Retain the data only for the period of time in which it is necessary.

**Scrutiny.** Establish procedures to allow individuals to review their records and correct inaccuracies.

### The International Dimension

You probably noticed that two of the seesaws in Figures 3 and 4 are not balanced. This roughly reflects the situation in the US. The American public seems to be very sensitive to government prying into personal lives, but much less sensitive to similar invasion of privacy when it comes from private organizations. This is reflected in data protection legislation.

Data protection laws may be classified according to three criteria:

- 1) the sector whose data bases are protected: only the private sector, or both the private and public sectors;
- 2) the manner of storage of data protected: only automated, or both automated and manual storage; and
- 3) the legal entity that is protected: only natural persons, or both natural and legal

persons, i.e. organizations.

Except for the American and Canadian acts, the laws apply to both the public and private sectors, i.e. both government and private organizations are subject to the same regulations of collection, maintenance, and disclosure of personal data. Over half the laws (including the US federal statute) encompass manual as well as computerized record-keeping systems. A minority of the laws apply to legal persons.

Many European countries have an institution called "Data Commissioner." Citizens can take their grievance to the Commissioner. The Commissioner then takes care of the complaint through negotiation with the organization or via prosecution in the court. In the US, it is the citizen who must take the case to court. Of the above list of measures to protect privacy, the European private organizations

must comply with many more items than their counterparts in the US. The disharmony of privacy laws has a grave impact on international trade. For example, Sweden does not allow the transfer of any personal data to the US, because privacy regulations in that country are much stricter than those in the US.

### Agenda for Research and Teaching

The following are suggested issues for study and teaching:

- 1) What data on individuals should and should not be collected?
- 2) What is legitimate or illegitimate in collection, maintenance, and dissemination of consumer data?
- 3) What is legitimate or illegitimate in the collection, maintenance, and dissemination of data by governments?
- 4) What should be the red lines in electronic monitoring in the workplace?

Figure 3: Balancing Government and Private Sector Needs with Individual Privacy Rights

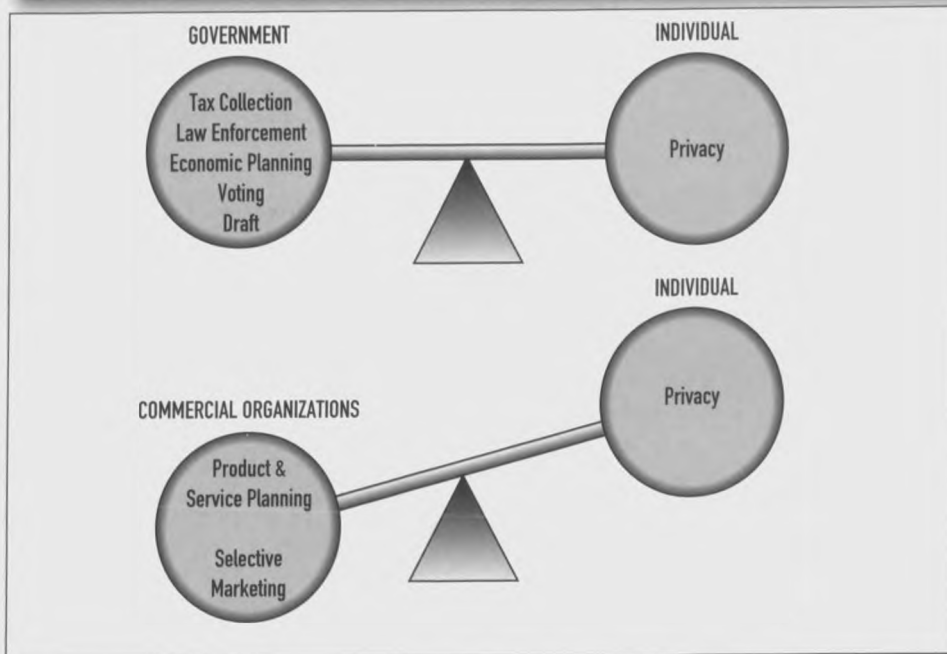
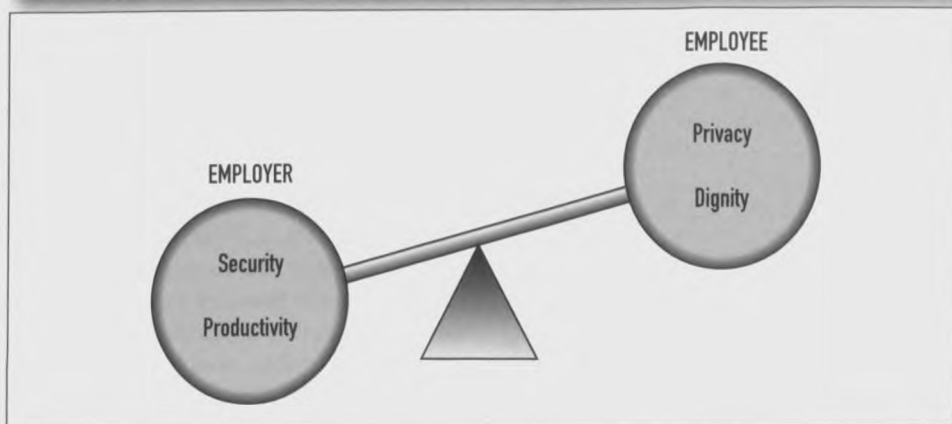


Figure 4: Balancing Employer Interests and Employee Rights



5) Should the individual be considered the owner of the data after it is in the hands of other parties? If so, what price should be attached to the holding and sale of such data?

6) How can privacy laws be harmonized internationally?

## COMPUTER CRIME AND PUNISHMENT

It would be redundant to teach a student that it is unethical and illegal to defraud a bank or destroy data through the use of a computer. These and similar acts are clearly criminal. However, there are many activities whose classification as crimes is questionable. For example, many of us believe that the launching of a computer virus should be criminalized. Indeed, several countries (e.g., the United Kingdom, Norway, and Germany) and US states (e.g., California, Illinois, and Wisconsin) have passed laws against such acts. But some IT professionals claim that launching a benign virus (e.g., the "World Peace" virus) should not be proscribed by law. They view such viruses as the exercise of free speech. What is the difference, they argue, between a benign picture of a christmas tree with holiday greetings popping up on your computer monitor and a commercial announcement popping on your television set? Neither is invited.

Hacking, a pervasive activity, is defined differently in the laws of different countries, and across states in the US. Some laws proscribe unauthorized entry into a "security computer system" (one to which a notice is attached which says who is authorized to use it). Others forbid any use of an information system without explicit permission. And some go as far as to criminalize even innocent, inadvertent entry. What is a just anti-hacking law? Viruses and hacking are just two examples that demonstrate the difficulty of computer-related legislation.

Determining punishment is not easy either. In their eagerness to quell hacking, legislatures have approved punishment such as forfeiture of the equipment involved in the crime. In several cases the equipment had served as a public bulletin board. Practically, there is no difference between an electronic bulletin board system and other information media, e.g., radio and newspapers. Would the police confiscate the press of a newspaper if an employee had used it to produce counterfeit money? To many this is violation of free speech.

Often, more than one party is involved and affected by activities performed with IT. Consider the above example. Even if the operator of the bulletin board system (sysop) is

found guilty, confiscation of the equipment denies many innocent people a source of information and a means of exchanging messages. Should we forgo their rights in punishing the culprit?

Unfortunately, the legal status of computer systems as means of dissemination and exchange of information is not as well established as those of telephony, paper mail, newspapers, radio and television. Hence, we still need to establish rules regarding protection of free speech and protection against government search and seizure (in the US, rights afforded by the first and fourth amendments to the Constitution).

### Agenda for Research and Teaching

The IT community should be involved in

*"It is imperative that we study ways to harmonize the codes of ethics in order to bring a single universal code up to the prominence of the Hippocratic oath."*

debating the above issues. The following are suggested research questions and teaching topics:

- 1) What behavior with IT should be considered criminal?
- 2) How can the government fight computer crime without violating the rights of innocent parties?
- 3) How can the government fight computer crime without violating basic civil rights, e.g., free speech and protection against search and seizure?

### PROFESSIONAL CONDUCT

Some ethical concerns have been resolved in the form of new, or amended, laws. Some will be addressed by future legislation. Yet, many issues will remain to be dealt with by the individual professional. Physicians, lawyers, architects, and other professional groups have adopted ethical codes. The emergence of the computer professional spurred the main organizations of IT professionals to draft their own codes.

All physicians solemnly swear to heed the Hippocratic oath. All lawyers in the same state, or country, vow to abide by the same ethical standards. However, not all IT professionals are bound by the same set of rules. The reason is simple: there is no legal certification of IT professionals. Certification is voluntary

at best. Many data processing professionals do not belong to any organization. Membership in a professional organization could, at least, make the member aware of the group's code of ethics. Worse yet, those organizations that have established codes of ethics have failed to collaborate and formulate one set of widely accepted rules.

The term IT professionals is loosely defined as programmers, systems analysts, computer operators, and managers in companies whose products or services are related to computers and computer networks. Unlike other professions, the IT professionals are very heterogeneous in qualifications and responsibilities. The work of some, e.g., systems analysts and project managers, involves decision-making. But others, e.g., programmers, do not make

decisions that affect clients. This makes the task of formulating codes of ethics for the profession difficult.

Each professional organization has adopted its own code. The Association for Computing Machinery (ACM), the Data Processing Management Association (DPMA), the Institute for Certification of Computer Professionals (ICCP), the International Federation of Information Professionals (IFIP), the Institute of Electrical and Electronics Engineers (IEEE) and several national organizations, e.g., the British Computer Society (BCS) and the Canadian Information Processing Society (CIPS), all have their own codes of ethics and professional standards. But parts of the codes are not coherent. In fact, on some issues the codes contradict each other. Except BCS, the organizations do not provide ethical guidance in addition to their codes [7].

Professionals have obligations to many different parties: the public, their employer, clients, colleagues, the profession, and their professional organization(s) [2, 12]. It is important to convey these obligations to students who will soon become IT professionals if we want them to be responsible practitioners. It is imperative that we study ways to harmonize the codes of ethics in order to bring a single universal code up to the prominence of the Hippocratic oath.

Also, the issue of mandatory certification should seriously be considered. Arguments for certification include assurances to the public that certificate holders are qualified to provide the services they claim they are able to provide. The revocation of a certificate would be a positive incentive to be honest and to keep one's knowledge abreast of technical development.

But there are arguments against mandatory certification. They include the claim that there are many different methods to develop computer programs, and there is no proven advantage of one over the others. A computer professional may be well experienced in one method, but not in other methods. It would be unfair to disqualify that individual merely on this basis. Another fear is that certification would create a guild. A closed shop tends to protect, if not foster, mediocrity of its members while excluding qualified people. It discourages competition and motivation for improvement because it enhances the status and income of those admitted at the expense of those excluded.

#### Agenda for Research and Teaching

The following questions are suggested for study and teaching:

- 1) Who should be considered an IT professional: only those in decision-making positions, or anyone whose training and work is in the broad realm of IT?
- 2) What would be the benefits and detriments of mandatory certification of IT professionals?
- 3) What are the elements that a universal code of ethics for IT professionals should include?
- 4) Should the codes, generally, prefer certain parties over others in case of ethical dilemmas (e.g., prefer the client to the employer, or prefer the public to the client)?

#### UNETHICAL USE IN THE WORKPLACE

Millions of employees use computers daily for their work. Some of the machines are "stand-alone," but many are linked to databases that hold information which is vital for their employers. The same computer that serves the employees for paid work may be used for personal purposes, or to access resources and data that are intended only for certain workers. Surveys show that only 40% of corporations in the US have policies regarding computer use. What is ethical and what is not in the use of computers in the workplace?

Many workers genuinely do not know where management draws the line, and often management does not have such a line at all. Using a company computer to run one's pri-

vate business may be considered unethical. But how about playing a game during lunch? Many companies do not object to recreational or educational use of their computers when the employees do it off company time.

A man who worked for the City of Indianapolis used the computer that the city rented to run his private business. He kept there lists of customers who purchased his dietary products. When his employers took the case to court, the court accepted the employee's likening of private use of the computer to employees' use of vacant shelf space to store their books, and to using their employer's telephone to make toll-free calls [1].

In another case, a computer systems manager for the Board of Education of the City of New York used his employer's computer to store and track race horse genealogies, to create a handicapping system for horse races, to compile and print his résumé, and for other personal uses. The City accused him of theft. A New York City Criminal Court found him not guilty. According to the law only stealing computer services from a commercial venture was considered a crime. The Board of Education was not a service for the public to hire. Also, the judge noted, the man had not stolen the computer time because his boss already had given him access to the equipment. It would have been different if the accused "plugged into a computer that was being leased to the public, and he was simply trying to avoid payment" (New York v. Weg, No. 1K023239).

These examples emphasize the need for policies in the workplace. Employees may unknowingly cause great harm to their employers if not cautious when handling information. Illegal copying of software by an employee subjects the employer to criminal prosecution. Unauthorized access to personal data of other employees or customers, too, may put the employer in an undesirable position at best or in court at worst. Managers in a Canadian bank found that employees sold computer reports to workers of another bank. They were not aware of the damage such information could cause when in the hands of a competitor.

#### Agenda for Research and Teaching

- 1) What is ethical or unethical of employers to include in their policy on IT use?
- 2) If the employer has no clear policy, what constitutes unethical use of IT in the workplace regarding:
  - a) copying of software?
  - b) use of IT not for the employer's gain but not for personal gain either?
  - c) use of IT for personal gain?

- d) use of electronic mail?
- e) access to personal information of employees, customers, and suppliers?

#### SOFTWARE: INTELLECTUAL RIGHTS AND DEVELOPER'S RESPONSIBILITY

Software is a unique type of creation. It is sometimes a form of expression, sometimes an invention, sometimes a product, and sometimes a service. Ethical concerns about software revolve around two issues. One is the ethicality of protecting the intellectual rights of the developer; the other is the responsibility of the developer toward the user.

#### Protecting Intellectual Rights

By law, developers of software may protect their intellectual rights in any of the following ways: as a trade secret, under a patent, or under a copyright. Since it is very easy to copy software, the first option is rarely used unless the software is not developed for mass marketing. The most popular alternative is copyright. Copyright laws have been augmented to include software. However, software is not printed text or music notes, nor pictorial designs or other "traditional" type of art work. Therefore, the courts have not been consistent in their interpretation of copyright laws regarding software.

In a landmark trial (Lotus Development vs. Paperback Software) a judge decided that the "look and feel" of user interface is protected and should not be copied without permission. Yet in another case (Apple Computer vs. Microsoft), the court decided that a user interface can be emulated by another developer. By and large, professional software developers seem to be opposed to copyright protection of user interfaces; however they support copyright of source code, object code, and computer-generated images [12].

The objection to software patents is even greater. Software developers overwhelmingly resent the idea that software of any kind be patented. Patents give their holder a much stronger monopoly than copyright. The idea of copyrights and patents is to encourage creativity and innovation that can benefit society by granting an individual or a corporation certain monopolistic privileges. Since a growing number of services, art works, educational material and other values are transferred in the form of software, it is important to strike a reasonable balance between the rights of the creator and the interests of the public.

#### Agenda for Research and Teaching (a)

Although there are voices against any copyright or patent protection of software, it is reasonable to assume that the public at large agrees to grant software developers some pro-

tection. The proponents claim that such protection made the US a world software leader. The protractors argue that software is different than other creations, and that protection discourages incremental improvement by small companies and individuals. The questions we need to answer are:

- 1) Should the government grant patents to software developers?
- 2) Should the government grant copyright to software developers?
- 3) If some protection should be granted, what types of software should be granted patents or copyrights (e.g., source code, object code, algorithms, user interface)?
- 4) Should the government devise special protection for software intellectual property that is weaker than patent but stronger than copyright?
- 5) Should software intellectual rights be protected for a shorter time than with copyright or patent to allow faster improvement to the software?

#### Obligations of the Developer

Faulty software may cause great harm. In fact, there are documented reports of injuries and fatalities caused by software [3, 9]. Courts usually refuse to accept claims such as "it's the computer's fault" when a client complains about bad service. The user of the software is responsible to the client. But it is not always clear to what degree the software developer is responsible to the user. It is appealing to argue that if the software is tailored especially for a specific client, the developer is responsible for defects. But if the client failed to communicate the requirements, should he not assume some of the responsibility?

In the case of "off-the-shelf" software, developers are not likely to be held responsible for damages caused by faulty software, to judge from litigated cases. But if, for instance, a contractor using an electronic spreadsheet bids too low a price because of defects in the software, shouldn't the developer be held responsible?

Different professionals may be involved in the creation of new software: project manager, systems analysts, programmers. Miscommunication and mismanagement may cause great financial damages [10]. In the case of knowledge-based systems, the expert providing the expertise for the system plays a major role. So does the knowledge engineer who translates the expertise into code. It is unclear who is responsible for what in such systems.

#### Agenda for Research and Teaching (b)

The creation of some software involves many parties. We should try to establish rules of responsibility when the software does not

function properly. The questions are:

- 1) In the chain project managers - systems analyst - programmer, who is responsible for faulty software?
- 2) What are the client's responsibility in communicating software requirements?
- 3) In the case of knowledge-based systems (e.g., expert systems), what is the responsibility of each contributor: the expert providing the knowledge, the knowledge engineer, and the eventual seller of the software?
- 4) Should government impose testing regulations, at least for software that may affect people's health?
- 5) If software testing should be regulated, what should the guidelines be?

#### WHAT THE FUTURE PORTENDS

Courts have found themselves in awkward positions when they knew a certain behavior was unethical but could not punish the culprit because the law lagged behind technological development. For example, unauthorized copying of information was not considered theft in the eyes of the law until just several years ago (and in many countries, still is not). Unauthorized copying of information does not deprive the owner of use of the information; and deprivation of use was an important element of the definition of theft. It took years until legislators adjusted existing laws or passed new laws to address the new reality.

To avoid ethical and legal gaps, public debate should start as soon as a new technology emerges. IT professionals and educators should play a major role in the debate. What is ethical or unethical in the use of a new technology should be considered today to avoid injustice tomorrow. Here are three examples of potential developments and concerns.

*Smart Cards.* Smart cards look like credit cards. They contain vast amounts of information about the holder. Some providers of health services already use them. The problem: an employee of the organization can put on the card information of which you are not aware and to which you do not have access because you lack the proper device that makes the coded information human-readable.

*The Electronic Immigrant.* Telecommunication enables commercial organizations to practically employ foreign workers without obtaining proper permission from immigration authorities. Technically, telecommuting is not limited to any territory. Problem: immigration laws may become useless against anyone who can render services via a computer. (This constitutes about 60% of the US work force and a similar rate in western Europe.)

*Teledemocracy.* It is predicted that in the foreseeable future telecommunication systems will be used for voting. IT may provide a modus for state-wide and national "town meetings" in which millions of citizens play a role in decision-making processes of national importance. The concern: how to ensure fair, untampered processes.


#### Agenda for Research and Teaching

IT professionals and educators know the potential abuse of information systems better than other groups in the population. If we study the issues now and make our students aware of the risks, society will benefit from the new practices and not be threatened by them. Here is a suggested agenda for research and teaching:

- 1) What new practices may we expect of existing IT by government, businesses, and individuals, and what may be unethical in such practices?
- 2) What future technologies may be used unethically by government, businesses, and individuals?

#### CONCLUSION

We laid out an agenda for research and teaching of current and future ethical concerns in the development and use of information technology. They are: underlying ethical theories, ethical versus legal treatment of the immoral behavior, privacy, computer crime and appropriate punishment, professional conduct, unethical use of IT in the workplace, software intellectual rights and responsibility of software developers, and consideration of future concerns associated with IT. As researchers, our task is to assess what is right and wrong in the development and use of the technology. This should be done by way of comparison to other technologies and media, but with attention to the special characteristics of IT. Perhaps the most appropriate research method is surveys, so that we can find what the IT professional community, as well as the public at large, consider ethical or unethical.

As educators, we are encumbered with the task to provide our students with appropriate tools to evaluate the conduct of IT professionals and other users of the technology. We must ascertain that our product, a well educated professional, is equipped not only with technical skills, but also with a solid moral foundation. The systems that these specialists will develop and manage will have a great impact on the lives of many people. Practicing ethically will help preserve some of the most important human rights. 



### **STATEMENT OF PEER REVIEW INTEGRITY**

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©1995 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, Journal of Information Systems Education, [editor@jise.org](mailto:editor@jise.org).

ISSN 1055-3096