STUDIA INFORMATICA 2003
Volume 24 Number 1 (52)

Joseph McRae MELLICHAMP
The University of Alabama

ETHICAL ISSUES IN INFORMATION TECHNOLOGY

Summary. In the paper, the ethical issues in informatics from sources of problems, through the human factor until solutions are presented. The ultimate purposes of information technology can be destroyed by computer crime, abuses, and invasion of privacy. On the other hand we can observed negative influence of the means and methods of information technology expressed by the complexity of the technology, the size of information technology organizations, and the phenomena of espionage, piracy and sabotage. The most interesting ethical issues in the information technology area fall in the category of human factors issues. The human factors issues – property rights, access, depersonalization, exploitation, reality, and artificial intelligence are discussed in details.

As a solutions of ethical behavior problems in information technology, the Gold-plated Brazen Rule and the professional tenets of the Data Processing Management Association Code of Ethics are discussed.

Keywords: computer crime, ethics, human factor, information technologies, network security.

ZAGADNIENIA ETYCZNE W INFORMATYCE

Streszczenie. W pracy przedstawiono zagadnienia etyki w informatyce w zakresie od źródeł kształtujących problemy poprzez wpływ czynnika ludzkiego do proponowanych rozwiązań. Najważniejsze cele stosowania technologii informatycznych mogą być zniszczone przez przestępstwa komputerowe, nadużycia oraz utratę prywatności. Z drugiej strony widoczny jest negatywny wpływ środków i metod informatyki spowodowany jej charakterystycznymi cechami w formie złożoności technologii, monopolizacji oraz zjawisk szpiegostwa, piractwa czy sabotażu. Najbardziej interesujące zagadnienia etyki w informatyce dotyczą zagadnień wpływu czynnika ludzkiego. W pracy szczegółowo przedyskutowano takie czynniki, jak prawo własności, dostępu do technologii, depersonalizacji, użytkowania, rzeczywistości wirtualnej oraz sztucznej inteligencji.

Jako podstawę rozwiązań problemów etycznych w informatyce przeanalizowano wykorzystanie tzw. Zasady Gold-plated Brazen oraz Kodu Etycznego zalecanego przez Data Processing Management Association.

Slowa kluczowe: bezpieczeństwo sieci komputerowych, czynnik ludzki, etyka, przestępstwa komputerowe, technologie informatyczne.

1. Introduction

A dozen years ago, I was asked by Richard C. Chewning, Chavanne Professor of Christian Ethics in the Hankamer School of Business at Baylor University, to write a chapter for a book he was editing [1]. My assignment was to identify and discuss ethical issues in two important functional areas of the business enterprise, namely, information systems and operations research. Writing the chapter allowed me to think broadly about the ethical issues in information systems and I realized that a similar work I had done four years earlier in the artificial intelligence field was simply one ethical component of the much larger domain – information technology [2].

Now this all happened over a decade ago. One would expect that with the incredible changes in technology we have witnessed in the last decade, there would also be a change in the ethical issues. Not so. The actors have changed and the specifics are different, but the dilemmas are not much different. Thus, for this paper, I will use the same categories that I used in the earlier version. Most of the examples and illustrations, however, come from the recent news. In fact, something I wrote several years ago to describe this talk is most appropriate, "Interest in ethical issues in information technology seems to be spurred by major headline-grabbing scandals." One doesn't need to go to the technical journals to read about ethical issues in information technology, it is all out there in the headlines of the daily newspapers because information technology affects each of us on a daily basis. Before we look at the various ethical issues, a few definitional comments are in order.

An *information system* is a system used to collect, store, process and present information to support the information needs of an organization (or individual). The term information systems is generally construed to imply computer based systems; hence such systems are the principal product of computer science and for organizations include the personnel and computer hardware and software committed to the task of providing information support for decision making. Obviously, we are talking of the whole array of *information technology* here – transaction processing systems, data warehousing, office automation, groupware, factory automation, decision support systems, artificial intelligence (knowledge based systems, neural networks, vision systems, speech recognition systems, robotics), electronic data interchange, the Internet, Web sites, etc.

Upon initial consideration, one is inclined to wonder if there are moral and ethical questions associated with activities that appear to be exclusively concerned with the accumulation and assessment of numbers, data, and facts. To be sure, there are many complex and perplexing issues. Addressing the concept of problem solving which is the objective of information systems, Joseph Weizenbaum wrote,

"Real problems in the real world involve, among other things, conflicts of interest among real people. They cannot be understood, let alone solved, without first understanding what goes on in the hearts and minds of people."[3]

In the same connection, Ron Howard wrote, "Since the formalism of decision analysis [information technology] is amoral, like arithmetic, any moral considerations must come from the people involved in the application [4]." Human involvement in the information technology field has opened the door to a host of moral and ethical considerations.

In the next section, we will examine these issues under three broad headings: ends related, means related, and human factors issues. The first category deals with issues related to the ends, or the intended and desired results, of information technology; the second category relates to the actions (means) and strategies, tactics, and techniques (methods) used to accomplish desired ends. The third category deals with those issues directly related to the human element. In the third section, we will consider some actual and potential remedies to the ethical issues in the field and show how these remedies require a biblical base. Finally, we will discuss some avenues for future research.

2. Ethical Issues

In the 1980's, AT&T conceived the concept of "the darkened data center" and actually did some preliminary investigation to demonstrate the feasibility of the idea. The darkened data center was to be a computer center that was entirely automated, eliminating the need for human involvement and the need for lighting of any kind as robots and other automated handling devices wouldn't require light. Of course, AT&T's interest in the concept was as a labor saving approach. It is interesting to speculate whether there would be ethical issues associated with such an automated system and whether or not information technology, in general, will ever become automated to the extent that ethical issues introduced by the human element will be eliminated or, at least, minimized. In the issues we will examine in this section, we will see that apart from human involvement, we would have little to report from an ethical standpoint.

2.1. Ends Related Issues

The ultimate purpose of information technology is to provide information to individuals and organizations for a variety of uses: communication, decision making, education, recreation, etc. Normally, we would consider the appropriate uses served by the information provided to be in some sense "productive" and "beneficial" for some segment or all of society, however we choose to define productive and beneficial. Unfortunately, information technology is not always used to achieve these stated ends.

1. Computer Crime. The proliferation of computers and computing technology and the simultaneous emergence of communication networks have created an environment in which a new type of criminal activity is flourishing. Rod Willis described the situation:

Along with giving managers [and individuals] instant access to information and making their jobs easier, it has made it relatively easy for a skilled bandit or dishonest employee with a personal computer and a modem to obtain confidential data – or millions of dollars – from unwitting companies, banks and government agencies [5].

The magnitude of this type of criminal activity is enormous. For example, two 18-year-olds were recently arrested in Britain on charges of breaking into nine e-commerce Internet sites in the United States, Canada, Thailand, Japan and the United Kingdom, stealing information on more than 26,000 credit card accounts, and posting some of it on the Web [6]. The FBI estimated that this episode could result in losses exceeding three million dollars. What is alarming about this is that similar examples appear in the news almost daily.

What makes this type of crime attractive to individuals? For one thing, it is fast – it only takes a few microseconds to do the deed. It is relatively safe – a skillful operator can make it extremely difficult to discover – and one is certainly unlikely to be shot or otherwise hurt in the act of commission. Prosecuting computer offenses is time consuming. The perpetrators are often very young and the victims are often large, affluent, impersonal corporations or agencies. Often, crimes are committed by disgruntled employees to get even with the bureaucracy – an employee who has been passed over for a promotion or denied a pay raise.

Abuses. Some information technology activities, while not violating existing legislation, do fall in the legal gray zones and might be appropriately termed abuses. For example, prior to legislation enacted in response to the stock market crash of October 1987, program trading, which is the practice of stock trading based on slight changes in stock prices detected by computer monitoring usually by large, institutional stockholders, certainly pushed the envelope of appropriate investment practice on Wall Street.

Perhaps the most flagrant example of this type of activity I've ever heard of was reported to me by a former graduate student who at the time was an executive of a large manufacturer of computing hardware. Apparently, a legal firm in California set up a computer system to monitor stock prices of large corporations. When the system detected a sizable loss in the price of a company's stock over some specified time frame, say 25 percent in a quarter, the law firm would contact all shareholders of the company and offer to initiate legal proceedings against the officers of the company for mismanagement. My student's company was the target of such an attack and actually ended up settling the suit out of court for approximately ten million dollars. Even though a shift in the market that resulted in declining demand for the firm's primary products was the principal reason for the slump in stock prices, my student said management decided it would be less expensive and damaging to his firm to settle than to fight the charge in the courts! While the law firm probably acted entirely within the letter of the law in pursuing these cases, most reasonable individuals would say that such behavior certainly offends the spirit of the law if not the ethical standards of the practice of law. This happened several years ago when the market was relatively stable as compared with today's market. It is not likely that the law firm is continuing to pursue these lawsuits.

3. Invasion of Privacy. George Orwell's classic, ***1984***, raises a specter that probably all of us have seriously contemplated in our imagination – the invasion of individual privacy by government. In Orwell's portrayal, the government (Big Brother) had listening devices in every home. These devices fed computer data banks so that every move or word was recorded and available for evidence, if necessary, for "population control [7]."

When Orwell wrote ***1984*** in 1949, such a situation was unthinkable, not only from a technological perspective but also from a human rights viewpoint. But what about today, how far have we come from the events depicted in this novel? "A lively discourse on the subject of Internet privacy has been boiling publicly for years. But the recent disclosure that an on-line advertising company, New York-based DoubleClick Inc., planned to use 'cookies' to wed profiles of individual Web surfers to their real-world identifications has heightened concerns. Some privacy advocates believe the only way for the Web to exist without a police state of regulation and legislation is to demand new 'opt-in' rules in which only those surfers who want to be tracked and profiled will be, based on a voluntary request [8]." In other words, the technology is now in place and being used to accomplish some of the very privacy we all fear.

2.2. Means, Methods Related Issues

We move now to issues related to the means and methods of information technology. They concern the complexity of the technology, the size of information technology organizations, and the phenomena of espionage, piracy and sabotage.

Complexity. In considering the whole area of information technology, one is immediately struck with the awesome complexity of the systems and procedures that are being developed. The Internet, for example, is a network of literally millions of computers worldwide. Software packages composed of hundreds of thousands of lines of code are common. How can any one company or consortium of companies ensure that such complicated and involved systems are developed without errors and will perform flawlessly? They can't. For instance, computer experts believe a two-year-old security hole in Microsoft's Information Server software allowed the British hackers access to the credit card information in the case cited earlier [6]. Given that it is not possible to develop software and hardware to standards of perfection, what constitutes acceptable levels of quality for technology products? What constitutes acceptable response from manufacturing firms or software developers when products don't perform in accordance with user expectations? Several years ago, a major chip manufacturer tried to ignore problems in the reduced instruction set of a new chip. Interestingly, information about the problem was broadcast over the Internet and in the face of mounting pressure from the information community, the company acknowledged the problem and agreed to address user concerns.

What is the best way to go about insuring acceptable quality standards for information technology products and services? Government regulation? Most individuals would not open this door. Public pressure on a case by case basis? This doesn't seem to be a very efficient way to proceed. Industry standards? How would such standards be set? How would you ensure that all organizations follow the standards, especially considering the international scope of involvement? These are difficult questions. They need to be addressed.

2. Monopolies. At this writing, Microsoft Corporation is in the news daily attempting to deflect an antitrust judgment against it with an accompanying order to split into two or more separate companies. One corporate adversary when learning of the decision against Microsoft said, "The court's decision confirms what almost everyone in the world knows – Microsoft is a monopoly that has acted illegally [9]." Most people remember in the early 1980's when AT&T which was and continues to be a big player in the information technology arena was forced by the federal courts to divest itself of the Bell Operating Companies and Western Electric. What is the problem with monopolies? Are the interests of the consumer best served by strong competition in the marketplace? How can we ensure that there is strong competition without undercutting the prerogatives of entrepreneurs upon which the information technology sector so heavily depends?

These are also difficult issues. If you talk to a dozen users of Microsoft products, you are likely to get as many different responses as to whether or not Microsoft competes unfairly in the marketplace and whether software products are adversely affected by the competition or lack thereof. We have federal antitrust laws in place to guard against monopoly practices in business. Do these statutes work? Are lawyers and judges qualified to discern whether and when a Microsoft has overrun good economic practice?

3. Espionage, Piracy, Sabotage. These are old concepts; however, they have taken a different twist in the information age. Espionage is essentially an organizational perpetration while sabotage and piracy are usually accomplished by individuals.

Espionage. Espionage is the unauthorized use of one firm's technology by a competitor. The technology might have come as a result of an employee changing jobs, or from reverse engineering a product, or any one of a number of other ways. There is a fine line here between what is legal and appropriate and what constitutes improper use of another's property.

The recent history of computing is replete with examples of individuals and corporations operating in the gray zone between effective competition and outright espionage. For example, it is well known that the design for the first Macintosh personal computer was strongly influenced by technology that one of Apple's executives had seen at a Xerox research facility. Effective competition or clever espionage? Compaq and Amdahl are two of many companies that were very effective in producing "IBM compatible" hardware – Compaq making personal computers and Amdahl making mainframes. Effective competition or clever espionage?

Quite frequently patent infringement lawsuits make the news, most often involving a firm in the information technology sector suing a competitor for stepping over the bounds. Many awards have been paid in such lawsuits and probably just as many suits have been resolved in favor of the offending firm. Recognizing that there is a fine line between strong competitive activity and illegal use of another's technology and realizing that there are huge profit opportunities associated with these types of ventures, we can expect that from time to time well intentioned executives will get caught with their hands in the cookie jar and unscrupulous executives will get away with the goods.

Piracy. Piracy is the unauthorized use of software. Almost 27 percent of the software used by businesses in the United States was illegally obtained, according to a study by Microsoft [10]. Microsoft estimates that approximately 65 percent of the pirated software is used by small- and medium-sized businesses; home users only account for about 15 percent. Of course, this is just the tip of an iceberg of enormous proportions because piracy is an international problem. India and the Peoples Republic of China have been cited in recent media releases as being among the largest offenders internationally.

The Business Software Alliance, an industry lobbying group, collected ten million dollars in fines in 1998 from companies identified by its enforcement activities as using software for which they did not have licenses [10]. Unfortunately, offenders are difficult to detect; often necessitating an unannounced search of a firm's computing assets. Such enforcement activities are expensive and can create unfavorable publicity. Trying to do anything about foreign violators is practically impossible. The problem in the U.S. has reached such proportions that Microsoft has launched an anti-piracy media campaign. This is an interesting dilemma; you almost have to prevail on a person's innate sense of "fair play" to cause them to be above board, yet this would appear to be more of an organizational problem than an individual one. To whom in an organization do you appeal to play by the rules? Much of what goes on in individual organizations in the realm of piracy is probably unknown to those in authority in the firm's information technology area.

Sabotage. Sabotage is the intentional destruction of the information resources of an individual, organization, or numerous individuals and/or organizations usually by a single individual or a small group of individuals. Sabotage is usually accomplished by gaining access to a computer system through hacking or by worms or viruses. Millions of users worldwide were recently affected by the "Love Bug" virus, which apparently originated in the Philippines and rapidly spread to every continent [11]. Initial estimates of the damage caused by this virus were in excess of 10 billion dollars! At this writing, the perpetrators of the Love Bug virus have been tentatively identified, and efforts to prosecute them are in progress. Unfortunately, as is often the case, the individuals who are believed to have written the code are students and have no personal assets to offset any of the damage they caused.

According to experts, at any given time there are a "couple of hundred wild viruses out there, but some are relatively harmless or just posted on someone's server [12]." Companies that specialize in anti-virus programs have catalogued "tens of thousands" of viruses. As networks become more powerful, it is expected that viruses, worms, and hackers will create more, not fewer, problems for computer users. An obvious solution to mitigate the threat of destructive activities such as these is to produce secure systems – an option that could impose an overhead burden of perhaps thirty-percent of system capacity and billions of dollars of developmental costs. The U.S. Congress appropriated $1.75 billion for the current fiscal year for initiatives to protect the nation's key computers against terrorist attacks and untold billions – actual figures are classified – to enable the Pentagon to deploy offensive tools to "wage cyberwars [13]." We can only imagine what the term "wage cyberwars" involves.

2.3. Human Factors Issues

Perhaps the most interesting ethical issues in the information technology area fall in the category of human factors issues. Not many of us are overly concerned by the complexity issue or computer crime, but most of us are directly affected by some of the human factors issues – property rights, access, depersonalization, exploitation, reality, and artificial intelligence. Some of these issues have serious long-term implications for our society, as we know it; the answers we come up with in the short-term will impact our quality of life for years to come.

1. Property Rights. Prior to the advent of the Internet, property rights had very little connection with the field of information technology other than that associated with perhaps a

computer program or software package here or there. The Internet changed this dramatically. With the communication capability and connectedness afforded by the Internet, rights to *intellectual property* has become a big issue. Suppose, for example, I write a book or develop some instructional materials and post these to a Web site; to what extent do copyright laws protect me? If the book has a copyright, but the instructional materials do not, is there any difference in the level of protection to which I am entitled? Suppose I produce a musical score or a recording or a movie, am I protected from the possibility of these properties being transferred to the Internet and distributed to whomever over that medium? These questions are being hotly debated even now in technology circles and there are no pat, easy answers.

In December of 1996, representatives from the United States and 160 other countries who are members of the World Intellectual Properties Organization met in Geneva, Switzerland, to sign treaties that extend copyrights to the Internet and strengthen copyright laws in many foreign countries [14]. Our own government has passed legislation that makes it illegal to manufacture or sell products that circumvent technology to protect copyrighted materials in cyberspace. Copyrights, of course, form the economic foundation of the entertainment industry. Artists are paid royalties for authorized use of their materials. The Recording Industry Association of America estimates that international piracy costs American creators $15 billion a year in lost sales. When you add to this the lost revenue from unauthorized use of literary works, movies, and other kinds of intellectual property, the magnitude becomes staggering.

Are existing copyright laws adequate to protect creators of intellectual material? Apparently not. Surfing the Net to track down violators is not the solution either. There is a tension here between providing access to those who want to use these materials and protecting the interests of those who have created them. What can be done to protect creative individuals?

2. Access. Access to information technology has also become a complicated issue. It has impacts at the individual level and other societal levels. For example, consider two grade school children; one whose parents are professionals and have a personal computer linked to the Internet with a color printer and the other whose single parent is on welfare. When the one turns in a homework assignment researched on the Net and printed on the laser printer with color charts and diagrams and the other turns in the same assignment handwritten, with little research support; how should they be graded? Do we penalize one for not having access to technology? Or, consider third world countries, which do not have the technological resources, including information technology, of the superpowers; how can they ever expect to compete in the global economy? Do the *haves* have any responsibility for the *have nots* in either of these two cases?

Another interesting access question is gender specific. Do women have equal access to information technology? A recent report from the American Association of University Women suggests that girls are scarce in both computer classes and high paying technology jobs [15]. It isn't because machines make girls nervous or because they aren't good at math, says the report, it is because girls think computers are stupid and boring and that computer classes are populated by boys who haven't matured beyond the seventh grade – "adolescent boys playing killing games." The AAUW report found no barriers to women entering technology fields and, hopefully, over time more and more women will be attracted to the field [adolescent boys notwithstanding].

Depersonalization. I wrote the following about depersonalization in my 1990 paper [16].

"An unintended result of our computer driven information society is the depersonalization of life. Much of our interaction with business organizations is computer driven. We get our utility bills and department store bills from company-owned computers. We write checks and send them back to the computer. Our banking is computerized. We can make deposits, withdrawals, loans, and so on by interacting with a computerized teller. A computer diagnoses problems with our car; a computer tells us we have high cholesterol. And so it goes. We interact once a year with the federal government not as individuals but as SSN XXX-XX-XXXX."

It hasn't changed. If anything, things have gotten worse.

I don't recall that we had computerized answering machines in 1990. People today long to call a company and talk to a real, live person. Telecommuting has increased dramatically since 1990. I have a neighbor in Atlanta who works in Irvine, California. It is now possible to do most of one's shopping over the Internet. You can purchase clothing, groceries, books, medicine and drugs, videos, records, stocks, antiques, cars, airline tickets, and so on *ad infinitum* over the Internet. You can even consult a doctor, Dr. Koop, over the Internet. Technology has definitely created problems by depersonalizing our relationships and by separating us from one another. Much of what technology offers is good and makes life easier, but the loss of identity and community must be considered a downside of technology.

Exploitation. The Internet has become the leading distributor of pornographic material in the United States; one of the principal uses of the Internet is distribution of pornographic material. "Cybersex has gone beyond a flirtatious romp online for many Internet users, with more than 2 million users now considered serious addicts – people who chat or visit pornography sites so often it interferes with their off-line lives [17]." With more than 60 million Internet users, the National Council on Sexual Addiction and Compulsivity expects the number of addicts to explode. The ones who are already hooked are wrecking careers, marriages, and family lives. Experts say the primary cause is an increasing lack of face-to-face time.

Unfortunately, this traffic is not limited to adults. Our children are exposed to both pornographic material and predators as they use the Internet. ABC News reports that 19 percent of teenagers who use the Internet have received unwanted sexual solicitations [18]. A Vermont counselor described how he ventured into various sexual chat rooms to test the participants' responses. "When he identified himself as a 15 year-old boy in search of adult women, he was chastised and told to get out. But when he identified himself as a 14 year-old girl, one man – in a different state – said he would arrange to meet [the counselor] at her school [17]." It is bad enough when adults become addicted to this type of activity, when innocent children are exposed to it things have gone too far.

Trying to control or restrict pornography on the Internet is difficult if not impossible. There are some thorny freedom of speech issues involved; we have an ongoing debate in our society as to what constitutes appropriate expression in the various art and literary forms, but there is no clear consensus. Unless and until we can come to some agreement in these areas, people will continue to operate in the gray zones (or the dark shadows). Apart from the First Amendment issues, the sheer level of activity and the numbers of individuals involved makes any type of control a huge problem. How do you keep 2 million people from participating in these types of activities? How do you even identify who they are? Who is responsible? This is a challenging problem!

Real vs. Virtual Reality. One of the subtle affects of information technology is the blurring of reality that comes with it. Or, to put it another way, what is the difference between real reality and virtual reality? Where is the line? I picked up an issue of *Newsweek* a couple of months ago and read the following advertisement on the **Cyberscope®** page.

"HOT PROPERTY. Finally, a Family You Can Actually Control. Ever wish you could be a different person? That life didn't stink? Computer games can't help you, but you can vent your control issues with The Sims ($39.95; 800 XXX XXXX). This innovative game from Maxis lets you create virtual people, then watch and guide them as they live out their lives. You'll become obsessed with your Sims' every task – however trivial. Finding them jobs, washing their hands, preventing them from burning down the nice house you built for them, finding them dates. As if you didn't have enough problems in the real world [19]."

This would be funny if it weren't so serious. The point is people who spend hours every day in a virtual world begin to confuse what is virtual and what is real. They do become obsessed with things that happen in the real world, and sometimes attempt to solve real problems with virtual solutions. I believe that much of the teen, and adult, violence we are experiencing in our society can be traced to this phenomenon, which is peculiar to information societies.

How do you manage this aspect of life in a technological world? Virtual reality has many positive uses. We use virtual reality in education, to train pilots, soldiers, police, drivers, golfers, and hunters. It is obviously an important and essential element of entertainment. It is important that we utilize the positive contributions of virtual reality while recognizing the downside issues. We really must address this issue of helping people to differentiate between real and virtual reality so that they are able to compartmentalize the two.

Artificial Intelligence. When I wrote my paper, "The *Artificial* in Artificial Intelligence is Real," in March of 1986 there was a sense of euphoria in the artificial intelligence (AI) community. Consider some of the claims researchers were making. "The ultimate goal of AI research (which we are far from achieving) is to build a person, or more humbly an animal [20]." "A person is just a program, too, in a way. We are 'programmed by our experience.' A computer is a very slow, very spineless human [21]." "Anything humans can do, a machine will be able to do [22]." Have these aspirations changed in the 14 years since then? I think not. Consider the quote by Bill Gates in the introduction. As I pointed out in 1986, and reiterate here, these statements are either naïve or ill-considered, they lead to confusion for novices and people who are outside the AI field and have a mind numbing effect on experts within the field.

What are some of the dangers to which this type of thinking can lead? One of the participants at the Yale symposium gives a partial scenario.

"Because the mind was now in software, you could back it up on disk. If you knew you were going on a dangerous mission, you could save a copy of yourself. If you get killed, your friends could resurrect the copy ... with a short gap in memory corresponding to the time spent on disk ... not too high a price: a small interval of death in exchange for immortality [23]."

Most rational people would write this off as something from a science fiction film. When it is spoken by one of the top robotics researchers in the U.S., it is alarming. This comment led me to coin the expression, "Granddad on a Disk." We are all concerned about the escalating costs of health care, especially for the aging population of the country. Artificial intelligence offers a nice solution. When granddad begins to lose it mentally or physically, we simply download him to a disk. Then we can withhold medical care, knowing that when he expires, it doesn't matter. When we wish to see him or talk with him, we can simply load his disk and viola! We have granddad!

Far fetched? Yes. But, many of those in the AI community see this as one of the ultimate outcomes of artificial intelligence. The logical extensions of this are scary. This explains why Sir John Eccles thought most of the AI guys at the Yale symposium were "crazy."

3. Solutions

We have now identified a number of ethical considerations within the information technology field. As I have said on more than one occasion, these are difficult problems, which.

in most cases, are even now being debated in the public forum. Are there any solutions? Does the Christian worldview have anything to say about these issues? How could a philosophy written nearly two thousand years ago in an agrarian culture possibly offer anything to these debates in the technological culture of 2000?

Most people in the information technology field recognize the importance of ethical behavior on the part of everyone involved in the field. Because of this recognition, the various professional associations all have ethical codes, which they expect their members to affirm and practice. For example, the professional tenets of the Data Processing Management Association are shown in Exhibit 1. Notice that there is a section in this document that applies to the obligation of association members to society. Among other things, members agree to ensure that their work is used in "socially responsible ways" and to "support, respect, and abide by the appropriate local, state, provincial and federal laws." If every individual in the information technology field followed these two simple admonitions, many of the ethical issues we have surfaced would vanish or, at least, be greatly reduced.

Unfortunately, many people involved in the information technology field do not belong to professional societies, and, thus, have little to guide them with respect to ethical professional conduct. Many of the problems that arise in the field from hacking and viruses, an appreciable level of computer crime, and much of the piracy of intellectual and creative property are the result of high school and university students who have little contact with information technology professionals. Moreover, there are few assurances that a high proportion of information technology professionals will adhere to the ethical standards of their associations. So where do we stand? Is there any hope for achieving ethical behavior in the technology area?

Several years ago, Carl Sagan wrote an intriguing little piece for ***Parade Magazine***, which he titled, "Rules To Live By [24]." In the article, Sagan was casting about for a simple rule to govern behavior and relationships. It is well known that the most widely observed principle of behavior in American business is the Golden Rule, "Do unto others as you would have them do unto you (Matthew 7:12)." Many managers have cited this simple principle as their preferred guideline when dealing with employees and many workers have acknowledged that this rule embodies the essence of how they would like to be treated by their superiors. Mr. Sagan determined to find a "better" principle to use in guiding our lives – one, which could be shown mathematically to be superior to all others, so in the article he presented and discussed a series of simple strategies, starting with the Golden Rule and continuing to his preferred axiom. Here are his offerings:

- The Golden Rule. Do unto others as you would have them do unto you.
- The Silver Rule. Do not do unto others what you would not have done to you.

- The Iron Rule. Do unto others as you like, before they do it to you. (He who has the gold, makes the rules.)
- The Tin Rule. Suck up to those above you and intimidate those below.
- The Nepotism Rule. Give precedence in all things to relatives and do as you like to others.
- The Brazen Rule. Do unto others as they do unto you. (Repay kindness with kindness; evil with justice.)
- Tit for Tat. Always be nice on the first move, then follow the Brazen Rule.
- The Gold-plated Brazen Rule. Forgive others for bad behavior occasionally -- say 10 percent of the time, follow the Brazen Rule otherwise.

Mr. Sagan gave some interesting examples from history of individuals who followed the different rules, for, example, Martin Luther King, Jr. and Gandhi were proponents of the Silver Rule, thus, it is the basis for the whole nonviolent protest movement. We can all think of examples of people who followed one or the other of them. For example, I have had some superiors in the distant past who followed the Tin Rule and can think of some well known historical figures who have followed the Nepotism Rule.

According to Mr. Sagan, the Gold-plated Brazen Rule can be shown mathematically to be the optimum rule and this is, of course, a well-known conclusion of that branch of mathematical analysis known as Decision Theory. Since the Gold-plated Brazen Rule is mathematically superior to the other rules, it must therefore be the preferred rule in all situations and circumstances (according to Sagan), and we must all be remiss if we don't follow it in all of our dealings with others. What Mr. Sagan didn't point out in the article, either because he didn't realize it [hard for me to imagine] or because it would have been damaging to his argument, is that The Golden Rule is a *special* case of the Gold-plated Brazen Rule [emphasis mine]. If we forgive others for bad behavior all the time (100 percent) and respond badly none of the time (1 – 100 percent), we will be following the Golden Rule. Thus, if we elect to set the "forgiveness allowance" at 100 percent, we will be following a mathematically validated optimum principle. Thank you, Mr. Sagan!

Table 1
Professional Tenets of the Data Processing Management Association (DPMA) Code of Ethics

These standards expand on the Code of Ethics by providing specific statements of behavior in support of each element of the Code. They are not objectives to be strived for, they are rules that no true professional will violate. It is first of all expected that an information processing professional will abide by the appropriate laws of their country and community. The following standards address tenets that apply to the profession.

In recognition of my obligation to management I shall:

- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.

- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:

- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:

- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect and abide by the appropriate local, state, provincial and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:

- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest, and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Source: DPMA Headquarters. Updated: May 25, 1995.

Now how could any of this possibly apply to ethical issues in information technology? Here's how. If everyone in the information technology area would always follow the Golden Rule as a guiding principle, all of the ethical issues would go away. There would be no computer crime – I wouldn't steal from another because I wouldn't want him to steal from me. There would be no invasion of privacy – government officials would not invade my privacy, because they would not want me to invade theirs. There would be no viruses. Property rights would be secure. I would help the less fortunate gain access to technology because I would want them to help me if I were disadvantaged. There would be no pornography because people would recognize it as exploitation of another person and no one wants to be exploited. [We might have to work a bit on the virtual reality issue.]

One wonderful attribute that the Golden Rule has going for it is that it is amazingly simple. It is not a page long list of dos and don'ts. One doesn't have to memorize a code of ethics and constantly refer to it to determine which of the subpoints relates to the given situation. It is eleven simple words. Even the youngest child can understand the concept. Moreover, it applies in all situations. It is timeless. It applies just as well today as when Jesus offered it 2000 years ago in the Sermon on the Mount.

The problem, of course, is how to get hundreds of millions of people in many diverse settings and cultures to live their lives by an ethical principle, even a simple ethical principle. I submit that this is the major challenge facing our society today. It is not just in the high tech areas that we have ethical failures. We see them in all of life. On the highways. In high- and low-tech families. In business and government. In our cities, in villages. In churches, in synagogues, in temples, and in mosques. In nation to nation relationships. Everywhere we look, we see ethical failures. And we have tried all kinds of solutions. We have instituted every kind of control mechanism imaginable. They don't work. Perhaps we could try a return to civility.

4. Conclusions

We have seen that ethical concerns pervade information technology not because the ends or the means or methods of the technology are flawed, but because the people who create and use the technology are flawed. We have discussed a few of the ethical problems in the information technology area. Where do we go from here? Several areas for future research efforts occur. I have been interested in this area for a number of years and have been on the lookout for material during all of that time, but I'm sure I have missed things. There are certainly other important ethical issues that need to be brought to our attention. We need to do a better job of gathering statistics and measuring the magnitude of the problem. I have been away from the university for 6 years now. Those of you in the university need to initiate studies, collect and analyze data, and suggest solutions.

Information technology is assuredly a global proposition. We need to look at the cultural aspects of ethical issues in the field. Why is software piracy, for example, more of a problem in some countries than in others? Are there political and/or governmental features of the problem we ought to take into account? Do strong copyright laws in some countries (with weak or nonexistent laws in other countries) help protect the intellectual property rights of individuals? What can be done to obtain more nation to nation uniformity in this regard? What about third world countries? What are our responsibilities toward them? What can we do and what should we do to help them with access and development?

Finally, there is the education issue. Professional ethics is important. Ethics may indeed be the only solution to the problems we have discussed here. How do we instill ethical principles in the people who operate in the information technology area? How do we communicate to the second grader in the U. S., or in Asia, or in Africa, that using computer technology carries an important responsibility? The responsibility to act responsibly, to act morally, to act considerately. How do we turn a world culture, which pursues things to the exclusion of character, around? That is the challenge before us who are educators.

One last comment and I'm done. I'm sure that some of you are in agreement with my proposed solution to the problems of ethical failures in the information technology area. There will be many in the information technology field who do not agree. Many will scoff at biblical solutions to technological problems. Many will suggest that we need to pursue scientific solutions. We just need to do so with more energy and more resources. Before you discard a simple biblical solution, consider what Joseph Weizenbaum, former professor at MIT and one of the early pioneers in the information technology field, had to say on this point.

"It is not those of us who seek to understand the world from a number of different perspectives, including the scientific one, who prefer ignorance to knowledge. It is those who, blinded by their faith that science can yield 'full' explanations, prefer to remain ignorant of whatever knowledge other ways of knowing the world have to offer [25]."

REFERENCES

1. Chewning R. C. -ed.: Biblical Principles & Business: The Practice. Colorado Springs, CO: NavPress. 1990.
2. Mellichamp J. MR.: The Artificial in Artificial Intelligence is Real. An invited paper presented at Artificial Intelligence and the Human Mind, an International, Interdisciplinary Symposium, Yale University, New Haven, Connecticut, March 1-3, 1986.
3. Weizenbaum J.: The Last Dream. Across the Board, vol. 14, no. 7 (July 1977), pp. 34-46.
4. Howard R.: An Assessment of Decision Analysis. Operations Research, vol. 28, no. 1 (January-February 1980), pp. 4-26.
5. Willis R.: White Collar Crime. Management Review, vol. 75, no. 1 (January 1986). p. 26.
6. Sniffen M. J.: British Hackers Charged with Credit Theft Atlanta Journal, March 25, 2000. p. B4.
7. Howe I.: Nineteen Eighty Four Text, Sources, Criticism. New York: Harcourt, Brace & World. 1963.
8. Harrington M.: Crumbling Privacy. Atlanta Journal, March 26, 2000. p. P1.
9. Geewax M.: Microsoft: Judgment Day. Atlanta Journal, April 4, 2000. p. C3.
10. Clothier M.: Microsoft Spearheads Industry Campaign Against Piracy. Atlanta Journal, April 28, 1999. p. D8.
11. Meyerson B.: Love Bug' Clones Afoot. Atlanta Journal, May 5, 2000. p. A1.

12. Maher B. A.: Virus Detective Sees More Problems Ahead. Atlanta Journal, May 21, 2000. p. F6.
13. Glass A. J.: Cyber-terror Battle Plan Unveiled. Atlanta Journal, January 8, 2000. p. A4.
14. Dart B. Copyright Cops Hot on Trail of Global Internet Music Rustlers. Atlanta Journal, August 24, 1997. p. B8.
15. Reimer S.: Girls, Computers are Getting Along Just Fine. Atlanta Journal, April 30, 2000. p. D12.
16. Chewning R. C. -ed.: Biblical Principles & Business: The Practice. Colorado Springs, CO: NavPress. 1990. p. 171.
17. Lore D.: Siren Song of Cybersex Strengthens. Atlanta Journal, May 6, 2000. p. C1.
18. ABC News broadcast. June 8, 2000.
19. Newsweek. February 28, 2000. p. 12.
20. Charniak E., McDermott, D.: Introduction to Artificial Intelligence. Reading, MA: Addison-Wesley Publishing Company. 1985. p. 7.
21. Schank R. C.: The Cognitive Computer. Reading, MA: Addison-Wesley Publishing Company. 1984. p. 52.
22. Alexander T.: Artificial Intelligence. Popular Computing, vol. 4, no. 7 (May 1985). p. 66.
23. Letovsky S.: Ecclesiastes: A Report from the Battlefields of the Mind-Body Problem. AI Magazine (Fall 1987). p. 67.
24. Sagan C.: Rules To Live By. Parade Magazine, November 28, 1993. pp. 12-14.
25. Weizenbaum J.: The Last Dream. Across the Board, vol. 14, no. 7 (July 1977), p. 44.

Recenzent: Dr inż. Lech Znamirowski

Wpłynęło do Redakcji 27 marca 2003 r.

Streszczenie

System informatyczny jest systemem służącym do zbierania, pamiętania, przetwarzania i prezentacji informacji w celu wspomagania informacyjnych potrzeb organizacji i jednostek. Tutaj mówić będziemy o informatyce w całej skali stosowanych technologii – systemach przetwarzania transakcji, hurtowniach danych, automatyzacji biura, groupware (praca grupowa z komunikacją zapewnioną przez technologię współczesnych sieci komputerowych – e-mail, newsgroup, wideofony i chat), sztucznej inteligencji (systemy baz wiedzy, sieci neuronowe, systemy wizyjne, systemy rozpoznawania mowy, roboty), elektronicznej wymia-

nie danych, Internecie, stronach Web, etc. Obecność człowieka w obliczu stosowanych technologii stwarza problemy etyczne, które rozważono w pracy.

Najważniejsze cele stosowania technologii informatycznych mogą być zdegradowane przez przestępstwa komputerowe [6], nadużycia oraz utratę prywatności [7, 8]. Z drugiej strony widoczny jest negatywny wpływ środków i metod informatyki spowodowany jej charakterystycznymi cechami w formie złożoności technologii [6], monopolizacji [9] oraz zjawisk szpiegostwa, piractwa [10] czy sabotażu [11, 12, 13]. Najbardziej interesujące zagadnienia etyki w informatyce dotyczą zagadnień wpływu czynnika ludzkiego. W pracy szczegółowo przedyskutowano takie czynniki, jak prawo własności – *intellectual property* [14], dostęp do technologii [15], depersonalizację [16], użytkowanie zasobów Internetu przez osoby niepełnoletnie, np. w przypadku pornografii [17, 18], rzeczywistość wirtualną stwarzającą określone problemy przy powrocie do rzeczywistości [19] oraz sztuczną inteligencję [20, 21, 22].

Jako podstawę rozwiązań problemów etycznych w informatyce przeanalizowano wykorzystanie tzw. Zasady *Gold-plated Brazen* wychodząc z założenia, że zasada ta jest właściwa, bo potwierdzona matematycznie jako optymalna na gruncie działu analizy matematycznej znanej jako *Teoria Decyzji* z jednej strony, z drugiej zaś jako rozwiązanie problemów etycznych przedstawione w formie doktryny Kodu Etycznego zalecanego przez *Data Processing Management Association* (Tabela 1).

Adres

Joseph McRae MELLICHAMP, Emeritus Professor of Management Science, The University of Alabama, Tuscaloosa, Alabama 35487, USA.