Four Ethical Issues of the Information Age

Today in western societies more people are employed collecting, handling and distributing information than in any other occupation. Millions of computers inhabit the earth and many millions of miles of optical fiber, wire and air waves link people, their computers and the vast array of information handling devices together. Our society is truly an information society, our time an information age. The question before us now is whether the kind of society being created is the one we want. It is a question that should especially concern those of us in the MIS community for we are in the forefront of creating this new society.

There are many unique challenges we face in this age of information. They stem from the nature of information itself. Information is the means through which the mind expands and increases its capacity to achieve its goals, often as the result of an input from another mind. Thus, information forms the intellectual capital from which human beings craft their lives and secure dignity.

However, the building of intellectual capital is vulnerable in many ways. For example, people's intellectual capital is impaired whenever they lose their personal information without being compensated for it, when they are precluded access to information which is of value to them, when they have revealed information they hold intimate, or when they find out that the information upon which their living depends is in error. The social contract among people in the information age must deal with these threats to human dignity. The ethical issues involved are many and varied, however, it is helpful to focus on just four. These may be summarized by means of an acronym — **PAPA.**

Privacy: What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others?

Accuracy: Who is responsible for the authenticity, fidelity and accuracy of information? Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?

Property: Who owns information? What are the just and fair prices for its exchange?

Who owns the channels, especially the airways, through which information is transmitted? How should access to this scarce resource be allocated?

Accessibility: What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards?

Privacy

What information should one be required to divulge about one's self to others? Under what conditions? What information should one be able to keep strictly to one's self? These are among the questions that a concern for privacy raises. Today more than ever cautious citizens must be asking these questions.

Two forces threaten our privacy. One is the growth of information technology, with its enhanced capacity for surveillance, communication, computation, storage, and retrieval. A second, and more insidious threat, is the increased value of information in decision-making. Information is increasingly valuable to policy makers; they covet it even if acquiring it invades another's privacy.

A case in point is the situation that occurred a few years ago in Florida. The Florida Legislature believed that the state's building codes might be too stringent and that, as a result, the taxpayers were burdened by paying for buildings which were underutilized. Several studies were commissioned. In one study at the Tallahassee Community College, monitors were stationed at least one day a week in every bathroom.

Every 15 seconds, the monitor observed the usage of the toilets, mirrors, sinks and other facilities and recorded them on a form. This data was subsequently entered into a database for further analyses. Of course the students, faculty and staff complained bitterly,

feeling that this was an invasion of their privacy and a violation of their rights. State officials responded however, that the study would provide valuable information for policy making. In effect the State argued that the value of the information to the administrators was greater than any possible indignities suffered by the students and others. Soon the ACLU joined the fray. At their insistence the study was stopped, but only after the state got the information it wanted.

Most invasions of privacy are not this dramatic or this visible. Rather, they creep up on us slowly as, for example, when a group of diverse files relating to a person and his or her activities are integrated into a single large database. Collections of information reveal intimate details about a person and can thereby deprive the person of the opportunity to form certain professional and personal relationships. This is the ultimate cost of an invasion of privacy. So why do we integrate databases in the first place? It is because the bringing together of disparate data makes the development of new informational relationships possible. These new relationships may be formed, however, without the affected parties' permission. You or I may have contributed information about ourselves freely to each of the separate databases but that by itself does not amount to giving consent to someone to merge the data, especially if that merger might reveal something else about us.

Consider the story that was circulating during the early 1970s. It's probably been embellished in the retellings but it goes something like this. It seems that a couple of programmers at the city of Chicago's computer center began matching tape files from many of the city's different data processing applications on name and I.D. They discovered, for example, that several high paid city employers had unpaid parking fines. Bolstered by this revelation they pressed on. Soon they uncovered the names of several employees who were still listed on the register but who had not paid a variety of fees, a few of whom appeared in the files of the alcoholic and drug abuse program. When this finding was leaked to the public the city employees, of course, were furious. They demanded to know who had authorized the investigation. The answer was that no one knew. Later, city officials established rules for the computer center to prevent this form of invasion of privacy from happening again. In light of recent proposals to develop a central federal databank consisting of files from most U.S. government agencies, this story takes on new meaning. It shows what can happen when a group of eager computer operators or unscrupulous administrators start playing around with data.

The threat to privacy here is one that many of us don't fully appreciate. I call it the threat of exposure by *minute description.* It stems from the collection of attributes about ourselves and use of the logical connector "and." For example, I may authorize one institution to collect information "A" about me, and another institution to collect information "B" about me; but I might not want anyone to possess "A and B" about me at the same time. When "C" is added to the list of conjunctions, the possessor of the new information will know even more about me. And then "D" is added and so forth. Each additional weaving together of my attributes reveals more and more about me. In the process, the fabric that is created poses a threat to my privacy.

The threads which emanate from this foreboding fabric usually converge in personnel files and in dossiers, as Aleksandr Solzhenitsyn describes in *The Cancer Ward:*

> ". . . Every person fills out quite a few forms in his life, and each form contains an uncounted number of questions. The answer of just one person to one question in one form is already a thread linking that person forever with the local center of the dossier department. Each person thus radiates hundreds of such threads, which all together, run into the millions. If these threads were visible, the heavens would be webbed with them, and if they had substance and resilience, the buses, streetcars and the people themselves would no longer be able to move. . . . They are neither visible, nor material, but they were constantly felt by man. . . .
>
> Constant awareness of these invisible threads naturally bred respect for the people in charge of that most intricate dossier

department. It bolstered their authority." [1, p. 221].

The threads leading to Americans are many. The United States Congress' Privacy Protection Commission, chaired by David F. Linowes, estimated that there are over 8,000 different record systems in the files of the federal government that contain individually identifiable data on citizens. Each citizen, on average, has 17 files in federal agencies and administrations. Using these files, for example, Social Security data has been matched with Selective Service data to reveal draft resisters. IRS data has been matched with other administrative records to tease out possible tax evaders. Federal employment records have been matched with delinquent student loan records to identify some 46,860 federal and military employees and retirees whose pay checks might be garnished. In Massachusetts welfare officials sent tapes bearing welfare recipients Social Security numbers to some 117 banks to find out whether the recipients had bank accounts in excess of the allowable amount. During the first pass some 1600 potential violaters were discovered.

Computer matching and the integration of data files into a central databank have enormous ethical implications. On the one hand, the new information can be used to uncover criminals and to identify service requirements for the needy. On the other hand, it provides powerful political knowledge for those few who have access to it and control over it. It is ripe for privacy invasion and other abuses. For this reason many politicians have spoken out against centralized governmental databanks. As early as 1966 Representative Frank Horton of New York described the threat as follows:

> "The argument is made that a central data bank would use only the type of information that now exists and since no new principle is involved, existing types of safeguards will be adequate. This is fallacious. Good computermen know that one of the most practical of our present safeguards of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard. I have every confidence that ways will be found for all of us to benefit from the great advances of the computermen, but those benefits must never be purchased at the price of our freedom to live as individuals with private lives . . ." [2, p. 6].

There is another threat inherent in merging data files. Some of the data may be in error. More than 60,000 state and local agencies, for example, provide information to the National Crime Information Center and it is accessed by law officers nearly 400,000 times a day. Yet studies show that over 4% of the stolen vehicle entries, 6% of the warrant entries, and perhaps as much as one half of the local law enforcement criminal history records are in error. At risk is the safety of the law enforcement officers who access it, the effectiveness of the police in controlling crime, and the freedom of the citizens whose names appear in the files. This leads to a concern for accuracy.

Accuracy

Misinformation has a way of fouling up people's lives, especially when the party with the inaccurate information has an advantage in power and authority. Consider the plight of one Louis Marches. Marches, an immigrant, was a hard working man who, with his wife Eileen, finally saved enough money to purchase a home in Los Angeles during the 1950s. They took out a long term loan from Crocker National Bank. Every month Louis Marches would walk to his neighborhood bank, loan coupon book in hand, to make his payment of $195.53. He always checked with care to insured that the teller had stamped "paid" in his book on the proper line just opposite the month for which the payment was due. And he continued to do this long after the bank had converted to its automated loan processing system.

One September a few years ago Marches was notified by the bank that he had failed to make his current house payment. Marches grabbed his coupon book, marched to the bank and, in broken English that showed traces of his old country heritage, tried to ex-

plain to the teller that this dunning notice was wrong. He had made his payment he claimed. The stamp on his coupon book proved that he had paid. The teller punched Marches' loan number on the keyboard and reviewed the resulting screen. Unfortunately she couldn't confirm Marches' claim, nor subsequently could the head teller, nor the branch manager. When faced with a computer generated screen that clearly showed that his account was delinquent, this hierarchy of bankers simply ignored the entries recorded in his coupon book and also his attendant raving. Confused, Marches left the bank in disgust.

In October, however, Marches dutifully went to the bank to make his next payment. He was told that he could not make his October payment because he was one month in arrears. He again showed the teller his stamped coupon book. She refused to accept it and he stormed out of the bank. In November he returned on schedule as he had done for over 20 years and tried to make his payment again, only to be told that he was now two months in arrears. And so it went until inevitably the bank foreclosed. Eileen learned of the foreclosure from an overzealous bank debt collector while she was in bed recovering from a heart attack. She collapsed upon hearing the news and suffered a near fatal stroke which paralzyed her right side. Sometime during this melee Marches, who until this time had done his own legal work, was introduced to an attorney who agreed to defend him. They sued the bank. Ultimately, after months of anguish, the Marches received a settlement for $268,000. All that the bank officials who testified could say was, "Computers make mistakes. Banks make mistakes, too."

A special burden is placed on the accuracy of information when people rely on it for matters of life and death, as we increasingly do. This came to light in a recent $3.2 million lawsuit charging the National Weather Service for failing to predict accurately a storm that raged on the southeast slope of Georges Bank in 1980. As Peter Brown steered his ship — the Sea Fever — from Hyannis Harbor toward his lobster traps near Nova Scotia, he monitored weather conditions using a long range, single sideband radio capable of receiving weather forecasts at least 100 miles out to sea. The forecasts assured him that his destination area near Georges Bank, although it might get showers, was safe from the hurricane-like storm that the weather bureau had predicted would go far to the east of his course. So he kept to his course. Soon, however, his ship was engulfed in howling winds of 80 knots and waves cresting at 60 feet. In the turbulence Gary Brown, a crew member, was washed overboard.

The source of the fatal error was failure of a large scale information system which collects data from high atmosphere balloons, satellites, ships, and a series of buoys. This data is then transmitted to a National Oceanographic and Atmospheric Administration computer which analyzes it and produces forecasts. The forecasts, in turn, are broadcast widely.

The forecast Peter Brown relied on when he decided to proceed into the North Atlantic was in error because just one buoy — station 44003 Georges Bank — was out of service. As a result the wind speed and direction data it normally provided were lost to the computer model. This caused the forecasted trajectory of the storm to be canted by several miles, deceiving skipper Peter Brown and consequently sending Gary Brown to his death.

Among the questions this raises for us in the information age are these: "How many Louis Marches and Gary Browns are there out there?" "How many are we creating everyday?" The Marches received a large financial settlement; but can they ever be repaid for the irreparable harm done to them and to their dignity? Honour Brown, Gary's widow, received a judgment in her case; but has she been repaid for the loss of Gary? The point is this: We run the risk of creating Gary Browns and Louis Marches every time we design information systems and place information in databases which might be used to make decisions. So it is our responsibility to be vigilant in the pursuit of accuracy in information. Today we are producing so much information about so many people and their activities that our exposure to problems of inaccuracy is enormous. And this growth in information also raises another issue: Who owns it?

Property

One of the most complex issues we face as a society is the question of intellectual property rights. There are substantial economic and ethical concerns surrounding these rights; concerns revolving around the special attributes of information itself and the means by which it is transmitted. Any individual item of information can be extremely costly to produce in the first instance. Yet, once it is produced, that information has the illusive quality of being easy to reproduce and to share with others. Moveover, this replication can take place without destroying the original. This makes information hard to safeguard since, unlike tangible property, it becomes communicable and hard to keep it to one's self. It is even difficult to secure appropriate reimbursements when somebody else uses your information.

We currently have several imperfect institutions that try to protect intellectual property rights. Copyrights, patents, encryption, oaths of confidentiality, and such old fashioned values as trustworthiness and loyalty are the most commonly used protectors of our intellectual property. Problem issues, however, still abound in this area. Let us focus on just one aspect: artifical intelligence and its expanding subfield, expert systems.

To fully appreciate our moral plight regarding expert systems it is necessary to run back the clock a bit, about two hundred years, to the beginnings of another society: the steam energy-industrial society. From this vantage point we may anticipate some of the problems of the information society.

As the industrial age unfolded in England and Western Europe a significant change took place in the relationship between people and their work. The steam engine replaced manpower by reducing the level of personal physical energy required to do a job. The factory system, as Adam Smith described in his essay on the pin factory, effectively replaced the laborer's contribution of his energy and of his skills. This was done by means of new machines and new organizational forms. The process was carried even further in the French community of Lyon. There, Joseph Marie Jacquard created a weaving loom in which a system of rectangular, punched holes captured the weaver's skill for directing the loom's mechanical fingers and for controlling the warp and weft of the threads. These Jacquard looms created a new kind of capital which was produced by disembodying energy and skill from the craftsmen and then reembodying it into the machines. In effect, an exchange of property took place. Weaving skills were transferred from the craftsman to the owner of the machines. With this technological innovation Lyon eventually regained its position as one of the leading silk producers in the world. The weavers themselves, however, suffered unemployment and degradation because their craft was no longer economically viable. A weavers value as a person and a craftsman was taken away by the new machines.

There is undoubtedly a harbinger of things to come in these 18th century events. As they unfolded civilization witnessed one of the greatest outpourings of moral philosophy it has as ever seen: Adam Smith's *Theory of Moral Sentiments* and his *Wealth of Nations;* the American revolution and its classic documents on liberty and freedom; the French revolution and its concern for fraternity and equality; John Stuart Mill and Jeremy Bentham and their ethical call for the greatest good for the greatest number, and Immanuel Kant and his categorical imperative which leads to an ethical utopia called the "kingdom of ends." All of this ethical initiative took place within the historically short span of time of about 50 years. Common to these ideas was a spirit which sought a new meaning in human life and which demanded that a just allocation be made of social resources.

Today that moral spirit may be welling up within us again. Only this time it has a different provocator. Nowhere is the potential threat to human dignity so severe as it is in the age of information technology, especially in the field of artificial intelligence. Practitioners of artificial intelligence proceed by extracting knowledge from experts, workers and the knowledgeable, and then implanting it into computer software where it becomes capital in the economic sense. This process of "disemminding" knowledge from an individual, and subsequently "emminding" it into

machines transfers control of the property to those who own the hardware and software. Is this exchange of property warranted? Consider some of the most successful commercial artificial intelligence systems of the day. Who owns, for example, the chemical knowledge contained in DYNDREL, the medical knowledge contained in MYCIN, or the geological knowledge contained in PROSPECTOR. How is the contributor of his knowledge to be compensated? These are among the issues we must resolve as more intelligent information systems are created.

Concern over intellectual property rights relates to the content of information. There are some equally pressing property rights issues surrounding the conduits through which information passes. Bandwidth, the measure of capacity to carry information, is a scarce and ultimately fixed commodity. It is a "commons." A commons is like an empty vessel into which drops of water can be placed freely and easily until it fills and overflows. Then its capacity is gone. As a resource it is finite.

In an age in which people benefit by the communication of information, there is a tendency for us to treat bandwidth and transmission capacity as a commons in the same way as did the herdsmen in Garrett Hardin's poignant essay, "The Tragedy of the Commons," (subtitled: "The population problem has no technical solution; it requires a fundamental extension in morality). Each herdsman received direct benefits from adding an animal to a pasture shared in common. As long as there was plenty of grazing capacity the losses due to the animal's consumption were spread among them and felt only indirectly and proportionally much less. So each herdsman was motivated to increase his flock. In the end, however, the commons was destroyed and everybody lost.

Today our airways are becoming clogged with a plethora of data, voice, video, and message transmission. Organizations and individuals are expanding their use of communications because it is profitable for them to do so. But if the social checks on the expanded use of bandwidth are inadequate, and a certain degree of temperance isn't followed, we may find that jamming and noise will destroy the flow of clear information through the air. How will the limited resource of bandwidth be allocated? Who will have access? This leads us to the fourth issue.

Access

Our main avenue to information is through literacy. Literacy, since about 1500 A.D. when the Syrians first conceived of a consonant alphabet, has been a requirement for full participation in the fabric of society. Each innovation in information handling, from the invention of paper to the modern computer, has placed new demands on achieving literacy. In an information society a citizen must possess at least three things to be literate:

> One must have the intellectual skills to deal with information. These are skills such as reading, writing, reasoning, and calculating. This is a task for education.
>
> One must have access to the information technologies which store, convey and process information. This includes libraries, radios, televisions, telephones, and increasingly, personal computers or terminals linked via networks to mainframes. This is a problem in social economics.
>
> Finally, one must have access to the information itself. This requirement returns to the issue of property and is also a problem in social economics.

These requirements for literacy are a function of both the knowledge level and the economic level of the individual. Unfortunately, for many people in the world today both of these levels are currently deteriorating.

There are powerful factors working both for and against contemporary literacy in our organizations and in our society. For example, the cost of computation, as measured in, say dollars per MIPS (millions of instructions per second), has gone down exponentially since the introduction of computers. This trend has made technology more accessible and economically attainable to more people. However, corporations and other public and private organizations have benefited the most from these economies. As a result, cost economies in computation are primarily available to middle and upper income people. At the same time computer usage flourishes among some,

we are creating a large group of information poor people who have no direct access to the more efficient computational technology and who have little training in its use.

Reflect for a moment on the social effects of electronically stored databases. Prior to their invention, vast quantities of data about publications, news events, economic and social statistics, and scientific findings have been available in printed, microfilm, or microfiche form at a relatively low cost. For most of us access to this data has been substantially free. We merely went to our public or school library. The library, in turn, paid a few hundred dollars for the service and made it available to whomever asked for it. Today, however, much of this information is being converted to computerized databases and the cost to access these databases can run in the thousands of dollars.

Frequently, access to databases is gained only by means of acquiring a terminal or personal computer. For example, if you want access to the *New York Times Index* through the Mead Corporation service you must first have access to a terminal and communication line and then pay additional hook-up and access fees in order to obtain the data. This means that the people who wish to use this service possess several things. First, they know that the database exists and how to use it. Second, they have acquired the requisite technology to access it. And third, they are able to pay the fees for the data. Thus the educational and economic ante is really quite high for playing the modern information game. Many people cannot or choose not to pay it and hence are excluded from participating fully in our society. In effect, they become information "drop outs" and in the long run will become the source of many social problems.

PAPA

Privacy, accuracy, property and accessibility, these are the four major issues of information ethics for the information age. Max Plank's 1900 conception that energy was released in small discrete packets called "quanta" not only gave rise to atomic theory but also permitted the development of information technology as well. Semiconductors, transistors, integrated circuits, photoelectric cells, vacuum tubes, and ferrite cores are among the technological yield of this scientific theory. In a curious way quantum theory underlies the four issues as well. Plank's theory, and all that followed it, have led us to a point where the stakes surrounding society's policy agenda are incredibly high. At stake with the use of nuclear energy is the very survival of mankind itself. If we are unwise we will either blow ourselves up or contaminate our world forever with nuclear waste. At stake with the increased use of information technology is the quality of our lives should we, or our children, survive. If we are unwise many people will suffer information bankruptcy or desolation.

Our moral imperative is clear. We must insure that information technology, and the information it handles, are used to enhance the dignity of mankind. To achieve these goals we must formulate a new social contract, one that insures everyone the right to fulfill his or her own human potential.

In the new social contract information systems should not unduly invade a person's privacy to avoid the indignities that the students in Tallahassee suffered.

Information systems must be accurate to avoid the indignities the Marches and the Browns suffered.

Information systems should protect the viability of the fixed conduit resource through which it is transmitted to avoid noise and jamming pollution and the indignities of "The Tragedy of the Commons."

Information systems should protect the sanctity of intellectual property to avoid the indignities of unwitting "disemmindment" of knowledge from individuals.

And information systems should be accessible to avoid the indignities of information illiteracy and deprivation.

This is a tall order; but it is one that we in the MIS community should address. We must assume some responsibility for the social contract that emerges from the systems that we design and implement. In summary, we must insure that the flow of those little packets of

energy and information called quanta, that Max Plank bequeathed to us some 85 years ago, are used to create the kind of world in which we wish to live.

References

[1] Solzhenitsyn, Aleksandr I., *The Cancer Ward,* Dial Press, New York, New York, 1968.

[2] U.S. House of Representatives, *The Computer and Invasion of Privacy,* U.S. Government Printing Office, Washington D.C., 1966.

Richard O. Mason
Carr P. Collins Distinguished Professor of Management Information Sciences
Edwin L. Cox School of Business
Southern Methodist University
Dallas, Texas