Human and organizational implications of computer privacy

by JERRY M. ROSENBERG*

Polytechnic Institute of New York
Brooklyn, New York

ABSTRACT

The computer was created to serve man. With increasing reason serious questions are being raised pertaining to the potential misuse of the computer. Specifically, the issue of privacy has come to the public's attention as cherished liberties and psychological needs are gradually being eroded as the technology of the computer expands.

Recent discoveries have shown how men desiring power can utilize data for their own benefit, leaving the person intruded upon with little recourse, or for that matter, any knowledge of the invasion into his private world.

This paper identifies the many implications of loss of privacy on man's ego, dignity and general ability to cope with these forces. Failure to possess privacy can lead to withdrawal, loss of productivity, lack of confidence, physiological deterioration and other conditions of mental and physical decline.

A significant portion of this paper details the protections that can be incorporated, primarily technical, to preserve the balance between the need for society to know and the need of the individual to remain independent. The basic conditions for man's well-being are being tested along with the foundations of our governmental traditions.

At present, computers have an almost limitless capability to store, intermingle and, at the push of a button, retrieve information on persons, organizations and a variety of their activities, all without the knowledge of those involved. Even now, stacks of punched cards and tapes store statistics about us that we may not know exist. We might never escape in time or distance the bureaucratic machinery keeping tabs on us.

With present technical capability, it is possible to develop a composite picture of an individual that can be stored in a single information warehouse. Each year we offer information about ourselves which becomes part of the record. It is often scattered across the continent and is usually inaccessible except after considerable effort. It begins with our birth certificate and is followed by a series of medical notations. Early in life we are documented as an added income tax deduction by our parents. Then there is information on what high school, public or private, and what college, public or private, we attended. At school, records are made of our abilities, grades, tests of intelligence and attendance. For some, there will be car registration and driver's license, draft status, military service or Peace Corps. Then job history is recorded—working papers, Social Security number, a first job, our performance with each employer, recommendations, and references—all this makes an interesting dossier. Then perhaps, a marriage license, a home mortgage, and when children come, the cycle begins anew. Should we divorce, the court records will be added. These would increase should we be arrested, convicted or serve time in prison. And of course, when we die, a last footnote is made.

In our daily activities we leave behind a trail of records: the credit card carbon for a luncheon meeting, the receipt from the hotel where we spent last night, our airline ticket, the check we cashed in a city bank, and the bill for the toys we charged for our children. There are also government dossiers including tax returns over a number of years, responses to census questionnaires, Social Security records, passport files, and perhaps, our fingerprints and military intelligence reports. If we have worked for a defense contractor or for the federal government, there are lengthy files on us that may note our associations and affiliations.

Information is power. These records may at various times be of considerable interest to people inside and outside a specific government agency. Years after our birth, for example, an interested party may be happy to pay for information from our birth certificate which is officially confidential. And in a number of cities there are entrepreneurs who obtain and sell this in-
formation as well as hospital records, police records, immigration records, and so on.

Confronted with the erosion of his privacy, the individual American has until now had the consolation that all these files have been widely dispersed and often difficult to put together. It has been a time-consuming, expensive proposition to compile a sizable file on any individual. Giant computers with their capacity for instant recall of a great variety of available information are changing all this.

The evolution of computerized complexes without effective public participation and protest can have a serious impact on our democratic process. Under our present system, individuals are expected to make fundamental choices where the future welfare is at stake, as would be the case in an election. By alienating the people from the decision-making process, control of the computer technology is left in the exclusive hands of those in possession of organizational power.

The public itself should question the drift of these technologies. We should want to make certain that human dignity, psychological well-being and civil liberties remain intact. We should demand to know the precise nature of the information that will be stored and who will have access to it. The public has the right to know who will have the power to control the computers and most importantly, how confidentiality and individual privacy can and will be protected.

Liberty is never gained once and for all. It is forever in conflict with civilization—a conflict which has no clear-cut solution but which reappears in cycles, usually in different forms. Each succeeding generation must win it anew. Each must defend it against ensuing dangers. This is necessary because we are constantly changing our life environment; society may be altered so frequently that safeguards that in the past adequately protected our liberties become obsolete.

Science and technology are of immense benefit to society. These advances are so important to us that we would not want under most circumstances to impede their movement in advancing our knowledge of the world. But they may also expose us to potential danger—to a pollution that could curtail our anonymity, solitude and privacy. Unless certain practices in the technological exploitation of scientific knowledge are restrained, they will cost us more than we should be willing to sacrifice.

And we must constantly evaluate these technologies which are tools developed to increase man's power to understand his world. The mere fact that an innovation presents itself does not mean that we should surrender years of experience and values to its authority. Yet it is difficult to bring social pressure to bear against the control of potentially dangerous technologies. One reason is that those who have the use of the technology are influential enough to prevent societal, or for that matter, legal restraints.

That privacy will forever remain because it is implied in the Constitution and Bill of Rights is not credible to the new adult population. With growing hostility toward the dominating technology and the establishment, a segment of this group fear that the documentation of their so-called acts of rebellion will only show that the freedoms once assumed have been surrendered. Should our older citizens in power fail to come to grips with the issue of preservation of privacy, it can be expected that the last struggle will be made by those who question how their present behavior, if documented, could be used against them at some future time.

The computer cannot be blamed for the loss of privacy. It is but an instrument created by man. Computers and other advanced machine systems are not permitted to be in error, but man is not a machine and does not have to be as efficient as the tools he has created to serve him. If man loses his right to be wrong, will he react by withdrawing from society? Will his curiosity to experiment with life falter? If this happens, man truly becomes nothing more than a machine.

Of course, not all computerized systems contain potentially damaging information. Some operations merely act as accounting systems and high-speed calculators, while others at more sophisticated levels are depositories for internal decision-making; some store research information from diverse sources; and some are documentors for the purpose of assimilation and distribution of pertinent data to a large community.

Not all computerized complexes contain the "sensitive" or potentially "threatening" information that might be found in a computerized system designed to collect personal data. But the possibility of incorporating such information does exist. Even the rather elementary, antiquated computer has the potential for being an information storage center. It doesn't matter whether it is formally called a "bank" or a "single unit processor"—any capacity to collect, store and retrieve data instantaneously upon request may, if misused, infringe on personal privacy.

There is little doubt that as computerized communications systems spread throughout the nation and world, surveillance by data processing is bound to increase. If the trend continues, it will soon be possible to have all personal information about an individual gathered on a continuous basis and held indefinitely until requested. The snowballing effect is quite pronounced here. When the decision is made to purchase a computer, more data are gathered about the employees, customers or taxpayers who are of interest to an organization. Although this may provide for better services, improved decision-making and policy-programming, it also provides personal information about individuals never known before the advent of computers.
ALONG THE ROAD TO PSYCHOLOGICAL SUBMISSION

Today man lives in an atmosphere dominated by the machine. He brushes his teeth with an electric toothbrush; prepares his meals with mechanical Toasters, ovens and broilers; works in an atmosphere of motors, switches, fans, typewriters; goes to and from home by car, bus and train; reduces the chores of home life with sewing machines, washing machines and drying machines. In the past only the craftsman used the tool. Today all of us take machinery for granted. As long as machines served us and did not threaten our rights as persons, we welcomed technology.

The charm of the horse-drawn buggy yields to the modern automobile; the candlestick maker is not needed in this day of electric power; the complexities of the abacus are incorporated into the computer's memory unit. Often we are glad to say goodbyes to what we leave behind because many innovations free man from monotony, physical effort and waste of energy.

Computers are part of this advance, aiding us in ways that are valuable for our everyday living and essential for progress on all levels. Much of what has been achieved in medical research and outer-space exploration would have been impossible without the wide range of sophisticated computers.

Unfortunately, sacrifices frequently accompany these changes. With all the splendid wonders of the computer we find ourselves asking: has man become submissive to the computers of today? Can each individual profess to be more human in his actions than the complex system he has developed to assist in daily endeavors? Will there be a growing tendency to create a world where we treat each other as machines? Are we building more barriers which prevent the individual from having the opportunity to evolve his own unique potential—to be self realized?

Man submits more and more as his ability to make choices about and control his future is gradually taken away from him. He is willing to have the machine make numerous decisions for him about his future; he is willing to permit the machine to build towers of brick and metal, hoping that it will not fail him when he has to live or work in them; he is willing to have the machine process his life's facts, hoping that it will be accurate and objective.

It seems that we are not aware of what is happening to us—that we are losing a little each day to the machines. We are usually too busy to think about matters which seem on the surface not to be so "important" as whether our cars are safe, or the price of bacon or the way taxes are skyrocketing.

What is most disturbing to the American population is the undemocratic process which starts at birth to make people believe that they are unable to say "no" to divulging personal information, thus perpetuating a collection of data that will follow them for the remainder of their lives—"frozen in time and the computer."

People want to determine for themselves in every particular situation of life just how much of their complex beliefs, attitudes and actions they choose to disclose. To the American, this data is more than just statistics. It is the data of judgment, a possible last judgment that can affect their schooling, employment possibilities, promotion, or role in the community. The citizens of this country want to have the right to a personal diary that is away and free from the organization's outstretched hands. They plead the case that if all their actions were documented, including their mistakes, it would be difficult to close a page of one's life and start anew. It would be a tyranny over mind and destiny.

To maintain their dignity and fill their need for psychic distance, people construct mental walls around themselves. To be a total psychic being, with stability and confidence, forces people to reject being intruded upon without permission. Psychologically, privacy demands a delineation of the self, the acceptance that each of us is unique and separate from all others. It recognizes an empathy toward the finer qualities within man. It demands the perpetuation of a private psychic domain, displaying a defensive shield against psychological penetration, unless authorized.

There is a growing antagonism against people desiring power, who will through mental coercion try to intrude upon our concealed thoughts. Unfortunately, we have learned that the man who wishes to gain control will employ various techniques to influence and force individuals and groups into submission.

People have a right to remain unique and different. But there are many, and indeed the number is growing, who intentionally or by title of their office, are against the solitary man. They may envy his uniqueness. They want to keep a close watch on his behavior so as to anticipate future moves, often defended in the name of science or national priority. They too often regard his privacy as a denial of their own mechanized psychology which has a stereotyped and oversimplified answer for everything.

COMPUTER COMMUNICATION AND PRIVACY PROTECTION

A major problem in protecting our privacy is that too often we believe in the principle that the ends justify the means. When we consider that the goal is the greater good of our people, we cannot understand why a specific intrusion should be prohibited. The result: gradual erosion of the value we place on individual privacy. Sometimes we are confused and become easily convinced that a particular device that may lead to personal intrusion is warranted on other grounds, such
as purposes of security. This is an inadequate argument, I believe.

As computer networks spread throughout the country and world, science and privacy must be able to thrive together. We will be collecting thousands of facts about everyone, depositing these details into the unforgotten computers of the future. To date there are no adequate legal protections to safeguard the individual against computer leakage. Furthermore, laws alone will not offer satisfactory protection in the face of widespread use of these systems. Although laws can impose penalties for violation and can set the limits of proper safeguards, legislative actions have not always been effective in the control of surveillance activities like wiretapping and eavesdropping.

There is reason to hesitate before passing new legislation that might in fact backfire. Laws that give special agencies or departments the responsibility of investigating those who break the law would be introducing yet other bodies that decide who can know what, thus putting a new decision-power in the hands of a few.

We have to make sure that information given to a specific organization will not be shared in such a way that the person's identity will be discovered. It is necessary to specify those who may use certain technological devices. Neither the principal of a school nor a personnel director should be allowed to enter at will the dossier on a potential or present student or employee. The question of duration of surveillance is most important. In addition, we need to determine what kinds of electronic devices are appropriate and permissible.

We must define the penalties that would be imposed on those who disclose information improperly or without authorization, and we must regulate the use of information for purposes other than those for which it was originally obtained.

We must also bear in mind that we are dealing with a super-technology that will become increasingly complex and difficult to evaluate. It is safe to assume that probably the only persons who will understand the complexities and operations of these systems will be the computer designers and systems engineers who are directly responsible for the evolution of the industry.

Safeguards can be inserted into a system in use, but it would be more efficient and less costly to build them in at the time the computer is designed. The burden of a great deal of the responsibility must lie with the computer manufacturers, if they want to avoid external regulations, they will have to start thinking about how to design systems with built-in safeguards.

To date, the best attempt to identify the relationships between computer surveillance and invasion of privacy has been outlined by Petersen and Turn of the Rand Corporation. They visualize two types of disclosures of information—accidental disclosures resulting from failure of the computer, and deliberate disclosures from infiltration of the system. They suggest countermeasures to prevent surveillance of data within a computerized system.

Unfortunately, essential safeguards are not as easily attained as is suggested by some of these outspoken specialists. It is one thing to design countermeasures as they apply to the "general" concept of computer leakage; it is quite another matter to build in protections for a specific computerized system.

For example, few can find fault with Petersen and Turn's countermeasures but they are merely a theoretical framework for the complex changes that are needed. These countermeasures offer little assistance to those attempting to design a surveillance-proof computerized system in the medical field, in an educational community, for a corporation or for a government repository. Examples of a specific computer utilization within a defined framework are necessary. The rules that apply for one computer installation might be inadequate for another or might fail to respond to the more crucial or pressing needs.

There are certain general rules of conduct pertaining to all computerized data centers that should be followed in order to increase confidentiality and reduce information leakage:

1. Let people know what their records contain, how they are used and protected, and who has access to them.
2. Employ a verification process to insure accuracy of data; in addition, permit the individual to review the data for accuracy, completeness, current application, and freedom from bias.
3. Categorize all stored information as intimate, private and therefore non-circulating (such as physical, psychiatric and credit information); pertinent, but confidential and having limited distribution; or public, and therefore, freely distributed.
4. Regard personal data as personal property, requiring permission for its use, and punishment for its improper use.
5. Appointing an ombudsman agency—or a committee that represents all levels of the organization—to take major responsibility for hearing and responding to complaints, and to determine appropriate measures to minimize leakage.
6. Record each request for access that is made, along with the authorization.
7. Make security checks on computer personnel.
8. Assess, from time to time, people's attitudes toward and anxieties about the issue of invasion of privacy. Such studies could be useful in determining what form of records would be most acceptable.
9. Periodically review and update the adequacy of the physical safeguards. Employ capable outside consultants to attest to the safety of the
systems used, and to assist in the development of appropriate technical devices (such as scrambled data and code names), and

10. Allow psychological seclusion and withdrawal from accountability to remain as a permanent stronghold of our value system. The individual must freely choose whether or not he wishes to become submissive to the power of the computer.

A creative response by the computer industry to its technology will probably serve, and satisfy, the public better than rewriting our laws. In fact, one can doubt that legal measures—although necessary—will be as effective as technological adjustments in the protection of the public’s privacy.

What is needed before the establishment of large computerized centers is a rigorous research effort to answer the following unresolved questions:

1. What are the purposes of a computerized central facility? What kinds of information are strictly relevant to these purposes?

2. How much information about an individual is required to guarantee that such services are useful to the person, community and nation? How accurate, objective and challengeable is the information?

3. What are the procedures for the sharing of the system?

4. How will individuals be protected from the creation and distribution of derogatory data caused by clerical mistakes or computer malfunction?

5. Will procedures be developed to permit individuals to see their files?

6. Will the cost of such a facility be justified in terms of future savings?

7. Will there be adequate safeguards to prevent penetration from the outside?

8. In whose backyard should computerized centers be physically established?

9. Will a computerized center officially created as a statistical system eventually become a storehouse of personal information? and

10. Does the concept of computerized communication centers suggest a changing value system and further intervention in the lives of Americans?

The burden of proof of the security of the data facility should lie primarily with those who propose it. They must demonstrate that they can create a virtually impenetrable and incorruptible system and justify its greater economy and expanding service.

The dialogue has just begun. The right to preserve privacy is a right worth fighting for. Events of the past several years clearly point to the need for a redesigning of our communications protections. Computerized systems offer great potential for increased efficiency; yet they also present the gravest threat of invasion of our innermost thoughts and actions. Transactions of our personal movement will glut the records and offer a very up-to-date picture of how we conduct ourselves in private. Some see this trend as leading to an Orwellian nightmare with Big Brother watching over us and reporting to the central record-control authorities any behavior adjudged out-of-line with stated policy.

We are slowly drifting into a world of nakedness. Each year an increasing number of technological devices invade the world that once we considered private and personal. In spite of this, we are still confident that our lives, activities, ideas, thoughts, and sensations are shared with no one unless we so choose. Will this confidence be perpetuated? Echoes of Watergate, CIA spying, domestic surveillance, wiretapping, etc. may well have shattered any future acceptance by the public. An uphill effort is required.

The snowballing effect of computers is very real indeed. The more you know, the more you want to know and the better your methods will become to get and integrate this information. In the end, will there be any place to hide?

Computers may continue to prove themselves the worthy servant of man. But the servant must yield to his master, and the necessary thought must be given to developing essential safeguards. The computer manufacturers have thus far shirked their responsibility, but they cannot long remain bystanders if they wish to continue to make their own decisions. Both the manufacturers and then the consumer must seek ways to control the all-documenting, all-remembering computer systems and demonstrate that machine technology need not necessarily bear the stamp of increased surveillance.

The ultimate submission must be of the machine to man. If we fail to act immediately to preserve our claims to anonymity, psychological independence and seclusion we may develop a permanent fear—a fear to enjoy the fuller opportunities of life. We will hesitate before experimenting with the challenges of the world. We could become carbon copies of one another—conforming, dull and psychologically equivalent to the computer—heartless and non-emotional.