COMPUTERS AND PERSONAL PRIVACY

Willis H. Ware

July 1977

P-5902

The Rand Paper Series

Papers are issued by The Rand Corporation as a service to its professional staff. Their purpose is to facilitate the exchange of ideas among those who share the author's research interests; Papers are not reports prepared in fulfillment of Rand's contracts or grants. Views expressed in a Paper are the author's own, and are not necessarily shared by Rand or its research sponsors.

The Rand Corporation
Santa Monica, California 90406

COMPUTERS AND PERSONAL PRIVACY *

It is a distinct honor for me to address a learned body such as the American Philosophical Society. My topic would not be called a learned topic; it is very much a real world problem and its solution is basically a matter of public policy and not in the findings of academic research. As I came here this morning by railroad from Washington, I reflected on the fact that I had not traveled by rail for perhaps a decade. The speed of special rail vehicles now appears to be about 25% faster, which by many measures is a significant improvement over 10 years or so.

If one looks at what has happened in transportation from the time that man started to walk to that of the fastest current jet, speed has increased from about a mile or two per hour to one or two thousand miles per hour--a factor of a thousand fold. Extending the argument to orbital speeds, there is another factor of roughly 10. As a technology to move physical objects from one place to another, transportation has progressed by an improvement factor of the order of 10,000. Parenthetically, it appears that there is not much further to go in terms of speed without major innovation. In contrast, if one looks at computing technology, the situation is just dramatically different. In the 30s when computing began to be done electrically, arithmetic operations were completed perhaps one or two a second. Contemporary machines easily function at millions of operations a second and some approach a hundred million operations per second; there is an improvement factor of at least a million in 40 years. Attempts have been made to project what improvement is left yet in the presently known art; estimates vary but with some confidence, the factor is between a hundred and a thousand.** Most computer specialists would agree that before the year 2000 computing technology will have progressed in speed by a factor of the order of 10^9 or 10^{10}--perhaps even larger. It is an astounding achievement.

---

*This talk was presented to the American Philosophical Society for Promoting Useful knowledge at their Annual Meeting's Symposium on the Computer and American Society, Philadelphia, Pennsylvania, April 22, 1977.

**The Ultimate Computer, W. H. Ware, Spectrum of the IEEE, Volume 9, No.3, pp 84-91, March 1972.

There have been corresponding improvement factors in terms of memory capacity, cost, and size. Appreciating as everyone does, what transportation with its thousand fold increase in speed has done to society, we ought not be surprised that computing technology has already dramatically impacted things. Transportation of the jet age has made us a mobile society; it has created many sorts of new services to support a mobile society; it has created new problems, some of them law enforcement. It enables us to have meetings or to take vacations wherever we please; it has even created a new biological phenomenon known as jet lag.

To further develop the argument, consider computing from another point of view. The correct perception of a computer is a device that applies a set of rules to a body of data; the set of rules is known as a computer program. If the rules are those of accounting and the data is financial, then the computer for all practical purposes will do accounting. If the rules are those of checkers and the data are positions on a board, it is playing the game. If the rules have to do with fluid flows, pressures and the behavior of chemistry, and the data are pressures and flows of a refinery, in fact the computer is running a refinery. If a body of data within a computer is information about people and the rules are those pertaining to maintaining and updating files, then the computer contains what has come to be called a personal data bank. It is a subject that has evolved into enormous public concern within the last 5 years or so and it is important to notice why.

The United States is a big country; there are 200-plus million people, each of whom leads a complex life. Our social institutions are big; government institutions are big; government runs large social programs and Congress insists that they be monitored for fraud, abuse and performance. Overall, it results in an unprecedented scale of recordkeeping that centers on information about people. If we did not have modern day computing technology with its ability to maintain records, its ability to store them cheaply, and its ability to retrieve them quickly, this country could not be what it is. We would literally have difficulty running a country of this magnitude with paper, pencil and green eye shades.

The issue that I want to address arises from the intersection of a demand in modern society for enormously improved recordkeeping processes and computing technology as being able to supply those recordkeeping processes. The subject

has come to be called privacy. While it had a documentary genesis in the early 70s with books by Alan Westin, Arthur Miller, and James Rule, computer people had been talking about the subject several years earlier. The computer industry and its professionals have been very responsible about the general impact of their technology and very responsive to society in trying to make sure that privacy and similar issues have been talked about, and something done.

A computer system that deals with information about people typically is the basis for decisions about them. It supports decisions made on such things as credit, a tax audit, welfare eligibility or payments, medicaid payments, insurance, employment. The circumstances that surround all such recording is quite unlike what would be expected. There is no right of ownership with regard to personal information; no one owns information that would be regarded as private and sensitive. Organizations deal with information essentially as the organization wishes; it is sold and bargained as an item of commerce; it is used freely for purposes of the organization--expedience, profit, whatever. We find the situation to be very one sided against the individual who really has no chips in the game. The organization holds them all and until quite recently, has played them as it saw fit.

In an unbalanced situation of this kind, there are obviously manifold opportunities for unfairness, for discrimination in unpleasant ways, and for harm. It is as though society had been using fire as a technology and had put a few fire departments around, but had not yet invented fire insurance and did not even realize the need for an arson squad.

The privacy issue became focused as a public policy matter in 1973 when the Secretary of Health, Education and Welfare--at the time Mr. Elliott Richardson--created a Special Advisory Committee on Personal Automated Data Systems that I had the privilege to chair. His motivation to organize it arose from a concern about the ubiquitous Social Security Number and the role it should play in the affairs of people. The HEW Committee--as it has come to be known--produced a report called "Records, Computers and the Rights of Citizens"* which was presented formally to DHEW and all of government in July of 1973. Then the action started. The concepts and to some extent even the words were the foundation for what is now known as the Privacy Act of 1974 (PL 93-579). The report has proved to be a definitive document and to have influenced much of what has happened in the world of privacy. What is this concept that has suddenly become such a visible public issue?

---

*"Records, Computers and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department Health, Education & Welfare, July 1973, DHEW Publication No. (OS)73-97. Available through the U.S. Government Printing Office, Stock Number 1700-00116.

Privacy is used in an information context. It does not allude to intrusion into one's physical, psychological or physiological space. Formally, it can be defined as follows: (1) It is the social expectation that the individual will have some say in how information about him is used, to whom it is communicated, and how it influences him; (2) It is the social expectation that the individual will have some protection against unwarranted harm because of the functioning of some recordkeeping system and be treated fairly by such systems; (3) It is the social expectation that the individual has protection against unwelcome, unfair, or intrusive collection of information.

There have been a number of legislative attempts to deal with some aspects of it. Some of them are well known, especially if one is a user of credit or credit cards. Present laws include the Fair Credit Reporting Act, the Fair Credit Billing Act, the Equal Opportunity Employment Act, the Equal Opportunity Credit Act and the Family Educational Rights Act. The first two are aimed at redressing difficulties that people have with credit-based systems. The next two are aimed at redressing difficulties that the country has with discrimination against groups; and the last one, against difficulty in educational recordkeeping. Each is a rifle-shot approach in the sense that it targets a problem and attempts to formulate solutions which are appropriate and pertinent to only it. The 1974 Privacy Act is quite different; it is an omnibus act that throws a very broad umbrella of behavior over federal agencies and gives to each citizen in the country certain rights. For example, any one can go to a Federal agency and ask to see a record maintained on him. Having seen the record, if there is reason to believe something is not correct, it may be challenged and the agency caused to reinvestigate, to correct it, and also to propagate such corrections to whomever has received the incorrect record. This is but one example of the provisions in the Privacy Act of 1974.

The private sector is not subject to the Act nor is state and local government except for Section 7 that pertains to the Social Security Number. The Privacy Act also created the Privacy Protection Study Commission of which I am privileged to be a member and also its Vice-Chairman. The Commission began in June of 1975 and was originally to end in June of 1977, but it has been extended to September, 1977. High on the list of concern had to be the private sector and an examination of its recordkeeping practices. The Commission has held hearings on most of the important recordkeeping areas in the private sector: insurance, credit granting, depository, employment, personnel, medical,

educational and others. On the basis of the hearings, we have developed an awareness of how the private sector keeps records and what the privacy risks are.

Let me give a brief summary of the thrust of the Commission report. The (DHEW) Secretary's Advisory Committee built its case around several principles: there should be no secret record systems; the individual has the right to see, to contest, have his record corrected; the individual has the right to prevent information collected for one purpose from being used for others without his consent; the recordkeeping organization has to assume responsibility for assuring that the record is complete, accurate, timely and relevant to the decision that is being made about the individual in question. The solution proposed by the Secretary's Committee was a Code of Fair Information Practices, the details of which I will not give. However, most of the things in the proposed code found their way into the 1974 Act. The Privacy Protection Study Commission has had a chance to return and examine the topic a second time. It will not be surprising that we have generalized and extended the snapshot of the situation that the Secretary's Committee perceived. While the HEW goals were directed mainly at the recordkeeping level of organization, we are trying to serve three major social goals,

- To minimize the intrusiveness of data collection
- To maximize the fairness with respect to the influence of record systems in making determinations about people.
- To create a legally enforceable expectation for the citizen that records about him will be treated as confidential information.

We will propose that our recommendations be implemented by a combination of voluntary industry compliance codes, amendments to certain existing laws such as the Fair Credit Reporting Act, by some new legislation, and by existing state-level regulatory mechanisms. In each of the areas examined, we will make specific recommendations. Not surprisingly, the individual should have the right to see his record and to a copy if he wishes; he should have the right to cause it to be corrected if he discovers errors in it. If there are errors that are corrected, the organization holding the record must propagate that error to whomever the individual asks to have it sent--in certain situations even to sources of data. Importantly, the individual must be fully informed at

the time of his first interface with the record system--what records will be kept about him, with whom they will be exchanged, how they will be used, how they will be verified and what other sources might be contacted in regard to them. When an adverse decision is made about an individual (for example, denial of credit) the individual must be told explicitly what items in the record have resulted in the adverse decision. Very significantly, we will not recommend an omnibus law for the private secor, an item that has been of concern to the private sector ever since the Commission began. We will try to achieve everything through a combination of industry compliance codes, amendments to acts, a few new statues and existing mechanisms.

For the Federal sector, we will recommend certain revisions in details of the present Act because there are operational difficulties with it. We have examined the compliance of Federal agencies in the 18 months that they have been subject to the Act and as one might expect, it has not worked perfectly. Rarely, however, does a complex subject get solved exactly right the first time, and thus, we will suggest revisions to improve matters in the Federal agencies. While the report was to be published on June 10, it is now due by the middle of July. At that time, it will be impossible to know whether the legislative process will pick up our ideas and carry them into law. My intuition is that there will be major new forward steps in privacy.

It is quite clear that when the Commission expires, the privacy issue will be far from finished. One part of it will have been taken care of, but there are important others. There is a whole spectrum of problems that could be called "public policy on information" that will need continuing attention by an informed public, by professional groups and by policymakers. I'll offer examples. In California, law provides that a hosptial owns its records. My name is on such records, but it is clear that the hospital does not own my name because I am still free to use it as I see fit. It is not ownership in the same sense as ownership of tangible property; there seems to be something different. In regard to information, one has to ask: what does ownership mean? Does it mean that one owns a piece of paper? Or does it mean that one owns a role of magnetic tape? Or is there some new concept of limited ownership? In a sense, the matter has already arisen as the country has attempted to re-examine its copyright laws.

A second example. An airline reservation system, an electronic bank terminal, and a point-of-sale system in the grocery market share an interesting common characteristic. Each captures information about some aspect of human behavior. In the course of doing the job it was designed for, it learns a lot about you. The airline reservation system knows where you travel, when you travel, whether you like first or coach class, whether you order special meals, and if so what special meals. An electronic fund transfer system knows practically everything about your daily and maybe even long term financial affairs. As credit cards become acceptable for more and more things (e.g., payment of traffic fines, payment of tolls, entertainment tickets), other aspects of personal behavior get into the record. The point-of-sale system captures a lot of information about individual behavior. Most have features for authorizing checks; thus it knows your bank, it knows when you were in the store, it knows what was bought; buying habits can be inferred. Soon an extensive body of information has accumulated, not because anyone intentionally started out to do so, but simply to do its job, the system had to gather it. The risk is this. Somebody will think of something to do with such a data base that is quite tangential to its original intent. Such collateral uses may be socially or individually distasteful, but there is no deterrent against the data holder's doing as he wishes.

The country may need special legislative action for data bases that have overtones of surveillance of personal behavior, movement or actions. There is precedent; the Fair Credit Reporting Act takes cognizance of a special body of information gathered about people for credit reporting matters. There is also the matter of transnational data flow in which it can move from one legal jurisdiction to another. Probably for a decade at least, there will be an ongoing public information policy that will have to be addressed.

There's another aspect of information policy that can be characterized by the phrase "tightening the processes of society." Think how many otherwise free decisions have been preempted because some record system exists. A minor example is multiple travel reservations to hedge a time uncertainty. Airline automated reservation systems make such things harder to do--an otherwise free choice has been preempted by the very existance of some recordkeeping function.

As record systems come increasingly to support decisions made about people--some decisions are already automatically made, for example in credit--identity of the individual and accuracy of establishing that identity becomes paramount.

If the identity of an individual is incorrectly established, then an improper determination may be made about him, or an unfair award made to him. Beneath this point is yet another crucial question: Is this country inevitably moving toward a universal personal identifier? Are we drifting toward what is called an enumerated society, in which everyone will carry an identity document that is unique to him and will identify him in any interaction where identity is important. The Social Security Number already is a de facto personal identifier, but there is a lot of very high emotion about its role in such a fashion. In the long run, the country will probably have the question of personal identifiers as a public information policy matter.

As we move forward to exploit the wonderful capability of computing technology and its ability to support the information demands of modern society and its institutions, we have to do so in such a way that the balance between all record systems and the individual is properly established. Obviously, if the individual is harmed or treated unfairly, we will not have done the job properly. As a final observation, the privacy issue has an interesting attribute that is perhaps unique; the country seems to be ahead of the game for a change. The analog of an environmental pollution problem has not yet happened in recordkeeping and we can all be thankful because had it been allowed to happen, getting on top of it would have been enormously difficult. After spending 200 years learning to run the country, it is rewarding to know that this time we did come out ahead.