PRIVACY: THE PRIVATE SECTOR AND SOCIETY'S NEEDS

Willis H. Ware

March 1975

P-5414

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

PRIVACY: THE PRIVATE SECTOR AND SOCIETY'S NEEDS

Willis H. Ware

The subject that I want to speak to is usually called privacy or some variation such as computer privacy. It is a term that means many things to many people. To some individuals, it is the right simply to be left alone; to others, it is the option to withdraw from an environment or to get lost from society. To yet others, it is the right to be secluded or not to be annoyed. Such variety of meaning creates difficulty when one tries to speak to the subject because communication may not be clear because of the semantic matter. We will have to be much more precise.

The issue before us is that of personal information contained in recordkeeping systems. It includes the way such information is used or abused, the possible impact of it on individuals, and the mechanisms that society will have to create to assure that no one is harmed in some way as a consequence of the operation of some recordkeeping system. While recordkeeping systems can equally be manual or computer-based, the major issue of concern is the computer-based one, in part because computer technology is a mysterious art to most of the population.

If one says that he is attempting to protect individuals against harm that might occur from misuse of personal information, immediately there are further semantic problems because one doesn't know what is meant by personal information nor by harm. It is to be noted, however, that the precise connotation of what is meant by harm and what constitutes personal information is a function of an individual's position in society. What is harm to one may only be annoyance to another. Such differences in perception of the issue plus aspects which are unique with each individual in part make it very difficult to deal with it in a neat way.

In this connection, it is very important to note the following matter. While it is easy for a professional group such as this to get together in a room and talk about privacy matters, we must not be deluded that we are a typical cross-section of society -- by no means are we a representative group. One issue that must be kept in mind as we struggle to accommodate this concept of personal privacy is this: Whatever solutions are conceived will have to be ones that work for all of society. They cannot be ones that are acceptable only to groups such as this because what one of us would be willing to cope with, and in fact might even find a challenge, would to another segment of society be an insurmountable obstacle. As professionals, we will have to keep in mind that our solutions must work for all of society. To underline the point, note that some 15% of society is judged to have an IQ less than 85; sociologists regard this segment of society as one that is just able to maintain a position and to take care of itself. As an absolute number, 15% isn't terribly big; but 15% of some 225 million population is some 30 million people, a group that positively cannot be overlooked.

What we as the U.S. population have on our hands is a very intricate social problem that concerns interaction between organizations that hold personal information about people and the people themselves. Obviously, the organizations that hold such information can be either public or private. Moreover, personal information, whatever it may mean to any one person, is a commodity that each of us feels very strongly about.

What is driving the problem? Why is it that the privacy problem has suddenly erupted when it has been latent for years? One thing that is driving the problem is the sheer size of this country; there are some 225 million of us more or less. Another thing that is driving the problem is the complexity of the life each of us lives. A third thing behind the problem is the expectation each of us has from government, and in particular the expectation that certain segments of society have from government. With costs escalating, the

drive for efficiency is important, and the concern about accuracy of personal records is an important driver. Collectively, these forces all add up to a very powerful trend that drives organizations to collect information about people for the daily conduct of business, for monitoring of social programs in the case of government, for conduct of research, for urban planning, for law enforcement, and many other purposes. While many of these are not new issues, what has taken the problem out of second gear and put it into overdrive, so to speak, is the appearance of computer technology that makes modern day recordkeeping possible. It would be wrong to imply that manual recordkeeping can be ignored; it cannot, but the computer-based aspect is what appears to frighten most people.

To constrain and particularize the discussion a little more carefully, examine for a moment what the notion of privacy means in the context of recordkeeping systems vis-a-vis the individual. Any one of us gives information to some recordkeeping system because he seeks in exchange some benefit. We give information willingly to an organization because we use it as a bargaining item to get from an organization something that we wish. It may be a benefit; it may be an opportunity; it may be some privilege; it may be some reward; but whatever it is, personal information about ourselves is part of the interaction process between us and an organization from which we seek something. Thus, I would argue that there is an implied bilateral concern between organizations and individuals that both parties have an interest in seeing that information is collected for its intended purposes, in seeing that information is used for intended purposes, and importantly, in seeing that individuals are not harmed by the use of such information.

The rub comes when organizations begin to use information for other purposes, ones that are not necessarily related to the motivation that prompted someone to give it. Moreover, such other purposes

are not necessarily in the best interest of the data subject. The classical example that bugs everyone is the sale of information that finds its way into a mailing list, an example of what to some people is regarded as harm but to others is simply annoyance. Generally, an organization makes a decision to use personal information with little consideration of the individual's interest; at least this has been the historical record. Yet other uses of information about oneself are not an aspect that was considered when that information was willingly provided.

In the interaction process between an individual and an organization, the citizen is in a significant one-down position. First, the personal information that has been given in most cases enjoys no legal protection; it is therefore subject to court seizure. One can find oneself in the public eye on short notice. Secondly, if one does choose to contest an organization and its use of information, our resources are small compared to the resources of a large organization; the game is a very one-sided one. Even if one does undertake the game, there is no good legal basis on which to seek redress of harm. The individual is on the short end of the stick when he stands himself up against recordkeeping practices of contemporary organizations.

The whole bundle of issues that we've talked around are collectively called privacy, or personal privacy, or invasion of privacy, or computer privacy or some other similar label. It is this collection of issues that the country is currently attempting to deal with by legislation. To put it into perspective, we, meaning society plus government, are attempting to achieve a better balance between each individual citizen and the totality of information or recordkeeping systems that surround him.

It is important to separate two issues that are commonly mixed up but that have to be distinguished. The first is computer security, a subject much talked about and to some extent, something done about. Computer security comprises three components: first, it is the

totality of measures required to protect a computer-based information or recordkeeping system -- including physical hardware, personnel, information and facilities -- against either deliberate or accidental damage from some defined threat. One does not attempt to protect against anything that the world might conceive, but rather against the threat that the system owners perceive to be relevant. Secondly, it is the totality of measures required to protect the system against denial of use by its rightful owners. An organization cannot afford the risk that an organized group of dissidents might pre-empt a computer-based record system and deny it to the rightful owners. Finally, it is the totality of measures required to protect information or data against divulgence to unauthorized users. The computer security job is largely a technical job overlaid with a certain amount of procedural and administrative matters.

In contrast, the second issue of privacy includes the measures to assure that an individual will not be harmed as a result of the operation of some recordkeeping system. One must notice that even though computer security safeguards get information only to authorized users with high assurance, the safeguards of computer security cannot control unauthorized behavior of the authorized user; this is one facet of privacy safeguards. The malicious user who seeks to steal information is presumably well fended off because the safeguards of computer security are intended to defeat the deliberate penetrator. The privacy issue is largely a legal matter because what one is trying to give the individual citizen is some control over the use of information that he has given, and to give him some mechanism whereby he can seek redress should harm occur.

Privacy in the computer sense is only one part of a much broader social issue that is developing quickly; it is part of the general social problem of society's struggle to achieve a proper balance with computer technology. One aspect of the matter is this: To what extent should an organization, either public or private, have the

right to make decisions for its own convenience and expedience when such decisions will strongly impact a major segment of the public? A prominent example is the proposed Electronic Funds Transfer System in which the financial industry is promoting a significant, if not dramatic, change in the conduct of financial affairs that will have impact on every person. From all appearances, however, the decision is being studied from the point of view of advantage to the financial industry; there seems to be little or no consideration for the point of view of society.

Interplay between technology and members of society is not new to be sure, but information technology is so pervasive throughout the affairs of our societal structure that it must be a more prominent social issue than ever heretofore. It seems imperative that we as a society and as a country will have to construct a mechanism to adjudicate and monitor situations of this kind. We cannot abdicate the decisionmaking process to organizations and permit them to do as they wish with regard to information systems that impact the public.

It is altogether too easy at this point in time to look back and note what the automobile industry and its related support industries have done to the country vis-a-vis pollution, but that is a hindsight observation. At the time, it is unlikely that anyone could have predicted the problem, but we all know that it has happened; we know that it is costly to recover from; and we know that it takes time to recover from an unnoticed problem. Let us hope that in the information business, we have learned a lesson from pollution, and that we do not dig ourselves into a hole that will be costly and difficult to escape from. It is to be hoped that in the privacy issue as manifested in such things as personal record-keeping systems and Electronic Funds Transfer Systems, we have matured enough to at least keep the hole shallow, so that with adroitness we can recoup when the problem bites us.

Against that background of privacy, its context, its position vis-a-vis society, let us consider next what is happening in the world about it. The dominant event in the last two years has been the Committee that was sponsored by the Secretary of the Department of Health, Education, and Welfare. You are familiar with the report that was produced: Records, Computers, and the Rights of Citizens.* Some 10-15,000 copies are in the world today, and have had a major influence in shaping legislative approaches to the problem. There are some points about the report that deserve emphasis because it helps explain what has happened subsequently. First of all, the Committee was chartered by HEW to look at the Agency's own problems, but as it turns out, the Social Security Number is also an HEW problem, and so it was included in the charter. Importantly, the Committee was not chartered to look at private industry. The recommendations of the group were responsive to its charter, and as such, were aimed primarily at suggesting to the Secretary of HEW what he should do internally with his own Agency; and secondly, how he should try to influence the Federal government from his position as a senior member of it.

The thrust of the Report was to give the citizen a better standing vis-a-vis the records so that he might assure himself that the information content is indeed correct. It attempted to give the citizen some measure of control by stipulating that agencies could not use information for other purposes without prior consent from the data subject. It established a legal basis for redress of harm by the citizen through the mechanism of law suits plus civil and criminal penalties. To stress again, however, the recommendations were always intended to be a report to the Secretary of HEW for action items by him. Specifically, the Report was not intended to be the

---

* No. 1700-00116, Government Printing Office, Washington, D. C. 20402; Reprinted by M.I.T. Press.

basis nor to provide exact words for draft legislation either at the Federal level or elsewhere. Very importantly, it never gave consideration to the private industry because very little of the testimony to the Committee came from private industry.

What has happened since the Report appeared was completely unanticipated resonance among the Report and what it said, the affairs of Watergate, and the genuine concerns and interests of several legislators. Within a month or two after the Report appeared, legislators not only in Congress, but in various states, picked the action items from it and used it as the basis for draft legislation. There are clearly several problems with that process. First, the words of the Report were not adequately examined to see if they were appropriate for draft legislation. Secondly, the Report did not apply to the private sector. Yet both things happened; whole sections of it were incorporated into draft legislation, and its recommendations were extended to the private sector. Eventually, all House and Senate action coalesced into one bill that was passed by Congress at Christmas time of 1974. On New Year's day 1975, the President signed into law what is now called the Privacy Act of 1974. It provides approximately what the recommendations in the HEW Report proposed. Among the states, only Minnesota managed to get a law enacted in 1974; others such as California and Ohio did try, but for one reason or another, the legislation was not successful.

As of the moment, there is a Federal Privacy Act, a Minnesota privacy act, and certain other state laws which deal with bits and pieces of privacy. In 1975, there are already three bills in or expected in California; there are roughly three dozen other states expressing intention; and there is an omnibus bill in Congress. The action is not all over by any means.

The present bill, the Privacy Act of 1974, becomes effective on September 27, surely a magic day in Washington. On September 28, consumer advocates may well be knocking on the door of various Agencies. The first suits may well be filed the same afternoon!

Importantly, the bill is public sector only, but it does apply to manual systems as well as to automated systems, and therein is a possible problem for agencies. The Act does seek to protect the individual by permitting him to examine his records as each citizen already has the same privilege under the Fair Credit Reporting Act. The individual can cause the record to be corrected if he finds it to be in error, and there is an elaborate process that he can go through in case he and the agency cannot agree on errors or corrections. The Act does require agencies to behave in a way that would be regarded as good. For example, they are supposed to collect only information that is relevant to the purpose in hand; they are supposed to collect information that is timely and up-to-date and relevant to the decisions that are to be made. Agencies must publish an annual notice describing in detail each of the information systems run by an agency, where each is located, who is in charge, where a citizen can go to complain, where one goes to see the record, what the data is used for, what class of users is served, where the data comes from, etc. If nothing else happens, the public ought to be able to get the government recordkeeping process out into view -- a non-trivial advance.

There is a mechanism within the Act that permits an agency to ask for exemption for some or all provisions of the law. It is a fairly complex mechanism, but there is an important aspect; namely, an agency cannot exempt itself from any aspect of the law without doing so in the public eye. In the federal government, there is a process called formal rule-making that requires an agency to publicly announce that it intends to establish some rule. The public has 30 days in which to object or submit views; if there are such inputs, the agency is obligated to hold a public hearing before implementing its proposed regulation. The exemption process works the same way, so the citizenry ought to know what agencies in government have exempted themselves from what aspects of the law and why. That also is a non-trivial advance because it lays a foundation for returning to Congress in the usual legislative process

and seeking changes that are deemed to be appropriate.

Something probably will happen to affect the private sector in the near future. The Act of 1974 provides for a Privacy Study Commission, one of whose chores is to look at the recordkeeping practices of the private sector and to make recommendations to Congress for appropriate remedial legislation. The life of the Privacy Commission is two years and starts when the last of the seven commissioners has been appointed. It seems unlikely that the Privacy Commission will be operational before the middle of 1975, so one would presume that at the end of FY77, there will be recommendations in Congressional hands for the private sector. However, a bill has already been introduced into the House by Representatives Goldwater and Koch for both public and private sectors -- H.R. 1984. Furthermore, many states have picked up the action items from the HEW report and used them as a basis for public and private sector draft legislation.

One cannot assume a priori that the remedial actions relevant to the public sector are necessarily the right ones for the private sector. There are many reasons to treat the two quite differently. One of the dominant reasons is that organizational and personal motiviation are so different in the public sector relative to the private sector; another is that the financial drive and motivation are so different in the public sector compared to the private one. We must not start out with the assumption that what has been done for the public sector is automatically the right thing to do for the private sector; unfortunately, that is exactly the way things are moving. While the situation at federal level hopefully will be a rational and sensible one, the state issue, and maybe the local issue, are other matters of concern.

If the fifty states do their fifty different things, it is very unlikely that there will be uniformity and consistency across their actions; moreover, the probability that the fifty states would act in unison is essentially zero. Any organization in interstate business would be faced potentially with responding to fifty different

sets of rules coming into effect on fifty different calendar dates. If that were to happen, any industrial or commercial entity in interstate business will be in a continuous state of retrofit; software stability will be a thing of the past and a dream.

Part of the problem is that a state level legislator is a different individual than a legislator at the federal level. Often, they are not full-time; often, they are not properly paid for the job they are asked to do. Since privacy is a viable white-hat issue, everybody is rushing to generate action. From the point of view of any individual, if our state imposes a bad thing to its own recordkeeping state-level agencies, at worst it can clobber the taxpayers of the state; but if the state legislates for private industry, the effects will spread beyond the state borders and the impact becomes profound.

The privacy safeguards that might be appropriate to the private sector need attention; here are some ideas. What are we trying to do? It would appear that the goal is forgotten, especially at state level. We are trying to get a reasonable balance between an organization and every individual so far as the recordkeeping interface is involved. One gives information to an organization for some purpose, and in return expects the organization to be socially responsible. It might not be, of course, or it might be careless, or it might be negligent; thus, the first aspect of a law for the private sector would provide the individual some legal basis for redress of harm just in case an organization weren't as responsible or as careful as it ought to have been. Redress of harm seems to be an essential ingredient. Significantly, there is a hidden agenda item on both sides of this point. The organization obviously wants to do whatever it has to do at minimum cost and the consumer wants the same thing because the cost of compliance will be passed back to the person as a consumer. Both sides have an interest in providing privacy safeguards at minimum or acceptable cost.

Secondly, one has given information to the organization for some purpose. The expectation is that it is to be used for that

purpose and not for some other, even though the other purpose might be revenue-producing. However, the stand needs to be weakened a little because the individual citizen probably will have to change his attitude and accept a relatively broad point of view on the acceptable use of personal information. After all, one interacts with an organization with the expectation that it will be there the next time needed; it is implicitly expected to have some continuity of existence. To remain a viable organization, it has to plan; it has to report things to the federal government; it has to conduct business properly; it has to make profits so that stockholders are happy; it has to do many things to stay in business. An individual must concede that such normal business requirements will necessitate use of information about himself. It seems inevitable that the general citizenry will have to take a somewhat more enlightened view about the use of personal information by the private sector than a view that might be appropriate to the use of personal information in the public sector.

The dominant aspect is that the private organization does not harm an individual by using information about him. Moreover, it should not annoy him by using information in a way that is not in the best interests of each person. If so, then let an organziation use information as need be. To put it another way, the citizen's expectation would be that the organization runs a clean operation, where the definition of "clean" would be a pragmatic one; namely, where, if a majority and representative set of affected people felt the organization was doing business properly, it would be accepted.

The implication behind such a position is the following. No system can be designed so perfectly that every possible case of potential harm can be accommodated and there be no anomalous behavior. The odds are against being able to structure recordkeeping systems that well. Therefore, the argument is: Let us design legislation that accommodates so-and-so percent of the problems anticipated. "So-and-so" ought probably to be 85 or 90 percent, some fairly large

number, but let us not pretend that anyone is smart enough to design legislation that will take care of 100 percent of the cases; we are not. Let us then conceive some general mechanism that will accommodate the rare cases that we have not thought of, or the ones that will materialize because the world always changes. In a sense, this is some kind of insurance-like mechanism that will take care of the things that one one is smart enough to think of a priori.

These are the goals to serve in private-sector legislation. What might be appropriate to serve them? Some kind of public notice appears appropriate. It need not be an annual one, and probably not even a public one; it certainly must describe the details of an information system to the "local universe," so to speak, the set of people which the system deals with directly. Why any notice? An open relation between a record system and the people it affects is good for the general health of the relation. Moreover, the openness of the relation will establish the credibility and social responsibility of the organization. Again, it is healthy. One might argue that everybody knows that an organization has this, that, or the other kind of recordkeeping system; but even so, there are 20 or 30 million people, at least, that we cannot necessarily expect to comprehend that. Let us not design systems that will satisfy us as a professional group to the exclusion of the rest of the world.

Probably one ought also to have access to the record and to have some mechanism that could assure that the records are correct for the intended purpose. It seems to be a wise thing, in part, to maintain a viable and credible bilateral relation. Ideally, there would be some constraint on what an organization asks of the data subject. It does not seem justified that any organization, public or private, have carte blanche shopping privileges to get everything out of the citizen that it thinks might be needed now or next week, or next month, or just in case. Some constraint on what is asked of the person appears desirable.

Finally, since no one knows how to deal with every case that might come along, it seems imperative to incorporate in private-sector law something that one might call a general broadly-based information liability. To characterize it by example, we all drive a car; and for that privilege we accept liability for damage that might be done with it. We protect ourselves in case it happens with insurance. An analogous kind of liability could be created to protect people who may be harmed by the operation or use of personal information; it would take care of the unusual or rare case in which somebody (for example) might be damaged because a Christmas card list was abused, or for any other dozens of examples that might be conceived. Such an "information liability" could function as a broad umbrella for straggler cases.

These few attributes are what seem appropriate to incorporate in private-sector legislation. Behind this point of view is the concept that a private organization should look on the use and protection of personal information exactly as it has been long accustomed to look at other risks of business. There seems to be no reason to treat it differently. Let an organization respond as it sees appropriate to privacy risks, but also let the organization be liable if it fails to assess the threat and thereby harms people.

Such minimal features are probably enough to keep the private sector in proper balance vis-a-vis its interface with the individual citizen. If compromise were unavoidable, a minimum starter package would probably include just some aspect of public notice or awareness plus a general information liability. Nobody will be able to solve the entire problem the first time, and so we ought to get started with safeguards that address the issue but do not overkill it. As we live with and learn about the issue, subsequent legislation can tidy up the things that have been overlooked.

We could probably all agree to the principles of what might be wanted in private-sector legislation. It is another matter to get the principles embodied into legislation in words that carry

out the intent of what has been agreed on. It is a tricky business to assemble words that are unambiguous, that are relatively clear of interpretation, that contain the right meaning, and that carry out a general policy that has been agreed upon before the fact. That is where present legislation tends to have problems.

At this juncture, note three components of responsibility that every one of us in this group has. First is the responsibility of each of us as a professional who practices a technology that just has to be one of the three or four most important ones that the world knows. It is we who can perceive the cost and operational consequences of draft legislation; it is we who have to implement the safeguards that legislation will ask us for; it is we who can provide the technological inputs that can contribute to sound legislation. Secondly, and again in a personal way, all of us belong to some organization, many of which have direct concerns with what would happen on the legislative front because it will influence the financial posture. Many, and perhaps even most, large companies are completely unaware of what is going on with regard to privacy legislation, certainly at state level and often at the federal level. Each of us as individuals can see to it that our respective company or our respective industry expresses its views on acceptable safeguards. But be cautioned. It will not do to express opposition to the cause of privacy; it will not sell. The privacy issue is so well established and has so much momentum behind it that it will not be turned off. The important contributions from the business industry are the constructive positive ones that move toward adequate and workable safeguards. Finally, each of us has the concern and responsibility of the person who has to live in a society that he has helped shape with his technology.

In the end, of course, what we all seek as a country, as a society, as a professional group, and as a government, is an appropriate balance between society and information technology as

we know it, practice it, control it, and develop it. The issue is far too important to be left to chance; we cannot back away from it and console ourselves that it will come out alright, because it will not. The issue needs to be steered to an appropriate point; it needs to be assisted by proper debate and by proper discussion from people and organizations who are equipped to provide it. SHARE collectively as an organization of importance and stature in data processing has an obligation also. Hopefully, it will and can respond and make its voice heard in the various legislative halls where the privacy issue will be thoroughly examined and discussed this year and next.