PRIVACY ISSUES IN THE PRIVATE SECTOR

Willis H. Ware

December 1977

P-6064

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 ISSUES IN THE PRIVATE SECTOR

Presented by
Dr. Willis H. Ware

The Rand Corporation
Santa Monica, California

Roughly a year and a half ago (when I first addressed GUIDE), the Privacy Commission was in the middle of its effort. On this occasion, I can tell you how it all came out, give you a keener insight into the whole matter and indicate the implications for you as individuals in the society, and as professionals in the data processing business.

To briefly review this subject, *privacy* is

a) the social expectation that an individual will be treated fairly by recordkeeping systems with which he must interact... or with which he must unavoidably interact because of the structure of society;
b) the social expectation that an individual will be protected against intrusive collection of information;
c) the social expectation that the individual should have a legitimate enforceable expectation that records maintained about him will be treated as confidential.

To put it in short phrases: the aspects of privacy are to

- minimize the intrusiveness of collection
- maximize the fairness with which information is used
- create a legitimate, enforceable expectation of confidentiality.

In contrast, computer *security* is

a) the totality of safeguards that are necessary to protect a computer-based system--its hardware, software, data, personnel, facilities, and all of its resources--to protect all components of that system against any harm;
b) that set of safeguards that assure that information from the system is divulged only to authorized users--the access control matter.

Obviously, security and privacy overlap; but, obviously also, privacy and security are different things. *Security* stops at the system boundary. One can draw a conceptual fence through the terminals, or the printers, or the card-readers and say "inside that fence is

the computer security job." The analogy is a little weak because there are communication circuits all over the country; one needs to include them inside the fence. Nonetheless, computer security concerns itself with what might be termed the "installation". In contrast, *privacy* is concerned with the use of information; and in particular, it is concerned with how authorized users of information use it to make decisions about people.

Partially, computer security is concerned with privacy because it assures that information goes where it is intended to go--to authorized users. Computer security erects safeguards against the deliberate penetrator, who attempts to pirate information from a system. Hence, computer security supports privacy--but computer security does not assure privacy. As the mathematician would say it, security safeguards are a necessary but sufficient condition for responding to privacy concerns.

Security is largely a technical matter with administrative and procedural collateral aspects. Privacy is a matter of organizational policy concerning use of personal information plus the legal environment that establishes public policy to define, constrain, and specify how information about people may be used in making decisions or determinations about them and governs some aspects of recordkeeping about them. While an organization may do a thorough job on security, it can fail completely on privacy.

The privacy movement commenced in the mid-60's when responsible computer people began talking about it. It advanced rapidly when the so-called "HEW Report"* was issued in early 1973. The report laid the foundation for contemporary understanding of privacy and also formed the intellectual foundation for the Federal Privacy Act of 1974. It introduced some essential new ideas: (1) a code of *fair information practices*--the notion that information ought to be used fairly; (2) according to a set of rules, the notion that there is a mutual interest between the recordkeepers and the record-kept--they who have the record and the individual about whom it is kept. There is a mutual interest of both parties to see to it that a record is complete, accurate, timely, and relevant; and used properly. The 1974 Act adopted these concepts and, to some extent, lifted words and phrases from the HEW Report for the law.

---

*Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education, and Welfare, DHEW Publication No. (OS) 73-97, July 1973.

In the deliberations prior to passage of the 1974 Act, one issue was: "Should the Act apply to the private sector as well as the public sector or, should the Act apply only to the public sector?" Resolution of that debate produced a Privacy Act applicable only to the federal sector, but which created the Privacy Protection Study Commission, whose principal job was to examine private sector recordkeeping and to answer the question: "What safeguards on privacy ought to be legislated for the private institutions of the country?"

The Privacy Protection Study Commission, born of Congressional compromise, was created by an act of Congress, not by executive order of the President. Written into law, therefore, was a time period over which it was to function, a budget under which it was to perform, and a rather lengthy prescription of exactly what it was to do. The Commission consisted of seven people--two appointed by the Senate, two by the House, and three by the White House. It had a good cross-section of professional skills and experience, and was supported by a very capable staff that averaged 25 in number. The Commission operated for two calendar years and 3 months at a budget of $1.75 million.

From my personal point of view as a taxpayer, the country has a real bargain in the Privacy Commission. It was a dedicated group that worked hard, long and very insightfully on the issue. It produced very relevant reports and appendices that will have a lasting impact on the privacy issue. The point is important because, if one examines commissions as an artifact of the Washington scene, reports get written and reports get filed, but action rarely happens. In the particular instance of the Privacy Commission, action will happen, partly because the issue is a live one and partly because the Commission has done a very outstanding job. I would challenge anybody to get done the research that the Commission completed in the time period and for its budget.

As stipulated by law, the report of the Commission was delivered to the President and to the Congress on July 12 of 1977. The members of the Commission and its senior staff did have a private audience with the President and received his assurance that he was familiar with our work, that he would carry the cause forward, and urge his Cabinet to do likewise. On that same day, a package of ten bills was introduced into the House "to give legislative expression to the work of the Commission."

The thrust of the Commission was focused quite sharply on the private institutions of the country. To quote the Act: The Commission was asked "to make recommendations to the President and to the Congress on the extent to which, if any, the details [of the 1974 Act] or the principles [of the 1974 Act] should be extended to the private sector." The 1974 Act was a broad blanket of behavior over all federal agencies and, hence, is an omnibus approach--everybody is treated the same. The dominant question facing the Commission, therefore, was: "Should the private sector be treated in an omnibus fashion with the same

omnibus bill?" The answer is of major importance, and transmits a very crucial signal to the private sector of the country. The bottom line of the Commission position is: "No--absolutely not. It would be wrong to extend the omnibus approach of the 1974 Act to the private sector." The reasoning behind it is important.

The Commission argued that the motivations of private sector organizations and their managers are very different from the motivations of federal agencies and their managers. It is argued that the record-keeping practices from one segment of the private sector to the next were so diverse and the needs so different that it would be virtually impossible to construct an omnibus set of safeguards that would do the job in each area but not unnecessarily impact some areas. In contrast, the agencies of federal government are very similar in their record-keeping needs from one to the next. The motivations of the managers are constrained largely by the political environment in which they operate. The organizations are not driven by the profit motive, as the private sector is. Therefore, the Commission concluded that there is enough difference between public and private sectors that the private sector should be dealt with sector by sector.

Our report,* is structured chapter by chapter on each of the record-keeping areas that we examined: insurance, consumer credit, commercial credit, medical records, education, banking, depository, etc. There is also a series of five supplements--one of especial interest.** Appendix 5 is called "Technology and Privacy." It reflects the Commission's effort to extrapolate forward thrust of types of technology that support record-keeping as well as to ask: "What are the implications for future record-keeping of the technology that is now available?" We did not try the "up, up, and away, blue yonder" approach of forecasting wonderful, new innovations that the computer art will produce; we simply said: "Given what is seen today, what will it mean for future recordkeeping?" To technologists, the fifth supplement is of particular interest.

In each area, the *modus operandi* was to conduct public hearings at which individuals and organizations were invited to testify; it formed the research data base. In such hearings, we tried to be perceptive of characteristics of recordkeeping, latent or visible abuses of information that might exist in each of them; and we tried then to conceive recommendations that would be responsive to the problems that we saw, area by area. Each of the several chapters in our report will take the reader through a discussion and description of the record practices of an area, to the problems in it, and to the recommendations that were conceived. Altogether, we proposed some recommendations spread across about a dozen or so areas. Of the areas, there are seven of direct concern to the private sector; the others are of concern

---

*_Personal Privacy in an Information Society_, Final report of the Privacy Protection Study Commission, Superintendent of Documents, U.S. Government Printing Office, Stock no. 052-003-00395-3.

**"Technology and Privacy," Appendix 5, U.S. Government Printing Office, Stock no. 052-003-00425-9.

to the government and deal with such things as confidentiality of tax records, government access to records about people, and research and statistics.

In any discussion of privacy, one is entitled to ask: "Is this a real problem or is it a group of people who have a white-hat issue to ride?" The Commission made a determined effort to find spokesmen that would stand forth and say: "Yes, I was harmed by a data system in the following way." It was able to surface a few such incidents; but, by far and large, such cases are difficult to find. When one does find them, people have a preference to not talk about it publicly. One cannot find in the Commission's "ten-foot shelf" of the record of its work, an exhaustive documentation of abuse of information about people. One will not find case after case after case of how this, that, or the other person or organization was harmed because information was used improperly. One will find a discussion of incidents, such as we were able to find them, but the important observation is that seven people who started to work together in June of 1975 and came from diverse backgrounds and tended to have much different views on privacy, over the course of two years working together, converged on a common viewpoint and conviction that: "Yes, the privacy problem is a real one for the society in this country and it must be attended to."

After the conclusion of the Commission's work, it occurred to me that there is another basis on which the privacy case can be made. I am almost willing to say that it is the dominant basis, although the Commission's report does not say it quite that strongly. One of the tenets of the privacy issue is trying to make sure that people are treated fairly by the record systems with which they must unavoidably interact. There is no way for any one of us to live in today's society without interacting with record systems; there just is no way. Not even a hermit on the top of a remote mountain could accomplish it; sooner or later, some survey-taker would come by. Therefore, as a consequence of existing in today's society, one cannot help revealing information about oneself in exchange for what is expected from society and its institutions. And what do we expect? We expect credit; we expect medical care; we expect education; we expect employment and all the other benefits of an affluent society. For each of them that we must have and must fulfill, information about ourselves will unavoidably be kept in records.

It is to your interest, to my interest, and to an organization's interest that such records be accurate, because accuracy of record is obviously a basic requirement for fairness of treatment. To reiterate, though, an accurate record will not assure fairness, but an inaccurate record will almost certainly guarantee unfairness. The privacy case can be made very strongly and simply on the argument that accuracy of records is of paramount importance for the fair treatment of an individual that participates in contemporary society.

I'd like to also make the following point about privacy by analogy. If the country does not solve the environmental pollution problem, the next generation and the next one after that and the next one after that will remember it acutely, because the lungs will still hurt and the eyes will still water and the houses will still be cold. There is a consequence of the environmental pollution problem that will carry forward and future generations will not be able to ignore it. In contrast, if the privacy problem is not dealt with now, there is a reasonable expectation that future generations will be raised in a different information culture with a different expectation; the privacy problem will conveniently get overlooked and forgotten. It is easy to convince oneself that, unless the privacy issue is dealt with promptly over two generations or so, it will vanish; we will find a dramatically different culture in this country. We will find a population that is completely enumerated, i.e., everyone has a universal identifier; we will find much broader use of information to constrain individuals' actions in undesirable or, perhaps, distasteful ways. New generations, having been brought up in a new culture, will accept it. Thus, there is no automatic carry-forward that will assure that the privacy cause will stay prominent in society. There is an immediacy about privacy that indicates we have to do it now.

Why do we have a privacy problem? We have a big country, 225 million people. We lead complex life-styles; we run huge social programs out of Washington and, properly, the Congress says that each has to be monitored and audited for not only financial responsibilities, but also for achievements. We have large private institutions, many of which maintain enormously large rosters of information on people. Large computer-based credit bureaus, for example, maintain records on 65 million people; Social Security Administration records on 200 million people. The numbers are big, and it is just not possible to run this country, with today's standard of living and the affluence that we all enjoy, with papers, pencils, and green eye shades; it is not do-able. One could not run the United States of today without computer technology; records are essential. There is no way to get along without records about people, but the questions arise: How are they used? How should they be used? How might they be used, and for what socially-acceptable purposes?

Obviously, records can be used in ways to harm people; records can be used in ways that are unfair to people; records can be used in ways that give rise to social discrimination. Imagine the computer version of what, in the real estate business, is known as red-lining, where one draws a line around a geographical area and says: "No, there won't be any loans inside that area." Imagine a computer scheme that does red-lining with much more sophistication and makes the decision of loan-or-no-loan based on many subtle social factors; how cleverly it could be used as a social discriminatory action. Sometimes, records will be used in ways that are just plain distasteful to society; for example, using the school records of children to track down and identify their parents for purposes of deporting them as illegal aliens. While

we might argue that such an activity is in the broad interest of society, by far and large, any of us would find it a distasteful use of records.

Records also play gate-keeping roles; it can be illustrated in terms of the Educational Testing Service at Princeton, New Jersey. There is no way that anyone of us can get into an institution of higher education without ETS providing scores on relevant tests. In a very real sense, ETS stands at the gateway between anyone and higher education. There are other examples; the same gate-keeping role clearly operates in the case of consumer credit.

The bottom line of this issue is that, in today's environment, personal information has no legal protection; organizations that hold it do with it as they wish. The individual has no standing to contest what an organization does with it. Organizations holding personal information have discovered--and one would anticipate they would--that information is a valuable commodity; it can be bought, sold, bargained, used, and can produce revenue.

Records are also shaping society in very subtle ways. Information is everywhere pervasive; every organization needs it to function. Everyone of us as a biological mechanism needs information to run. Information is everywhere and, computer specialists are a privileged group in that we have the only technology that can process information better than the human brain. In that light, consider the responsibility that rests upon us in such a pivotal position. The information question, if one can use that phrase, and the public policy on information that this country must develop ranks equally with energy in my mind as an issue to be addressed and addressed quickly.

In regard to the recommendations of the Commission, there are some 165 of them. As examples, consider some that cut across recordkeeping areas and use them to illustrate the consequences for ourselves and the environments in which we function.

How does one assure an accurate record? How does one exploit the fact the subject of a record is a player in the game? Obviously, one permits the individual to see it and to take a copy of it with him. One permits him to challenge facts in the record or to challenge its incompleteness or its timeliness. If he persuades the organization that "Yes, there's an error", or "Yes, there's something missing", or "Yes, there's something that's stale", then there must be an obligation on the organization to correct the record. If a record has been disseminated to third parties (and most of them do migrate from place to place), then there is an obligation on the institution to promulgate corrections to recipients that have in the past received the record with an error in it. That theme--to see and to copy, to challenge, to contest, to cause to have corrected, to cause to have corrections promulgated--infuses all the areas in which the Commission has made recommendations. The idea is expressed in different words in insurance, consumer credit, depository medical records, and others, but the concept is pervasive.

In some areas, apropos of the intrusive collection aspect of privacy, we have taken the position that some methods of collecting information are inappropriate and should be proscribed. The methods in question are inappropriate in that, when used, the individual is deprived of any control over revealing information about himself; an obvious example is the polygraph and another, the psychological stress evaluator, which listens to a voice and allegedly determines on the basis of its intonation and content, whether one is being truthful or not. Another obvious example is the pretext interview, in which an interviewer conceals his true identity and true purpose, and concocts some story in order to tease out what he really wants to know, except that the interviewee does not realize what is really happening. In any one of the examples, the individual has been deprived of any control over what he reveals about himself. The Commission has taken a very strong stand and agreed with the views of Congressional committees and said, "Such practices are inappropriate information practices, and should be discontinued."

There are other recommendations which collectively establish what can be called institutional behavior, an obligation on the institution to see to it that records are accurate, timely, complete and properly used; records are protected as confidential and that the institution take affirmative action to make such things happen. In addition, an institution must not share records at the casual request of an enforcement individual who appears in person, but rather insist on the formality of the judicial subpoena process.

Much of what privacy is all about and much of what it takes to respond to privacy is, in fact, what anyone would call sound information practices. We, as professionals have, in fact, allowed information systems to come into being which do not always reflect such sound information practice. For one reason or another, we have cut a corner in one way or another, we have been unsuccessful in persuading management to give us quite enough budget to do the job right. Moreover, the field simply has not matured to the point where we have well established guidelines nor preferred practices on how to do things right. For a variety of reasons, there are many information systems that simply do not reflect sound information practice. Much of what will be required to respond to privacy legislation is simply tidying up sloppy situations that have been allowed to happen.

Where do you and I stand as data processing professionals, holding in our hands the technology for information? Let me suggest an analogy. It is the mid-1930's. We are trying to project that in a few decades there will be untold acres of the country covered by macadam and concrete; there will be tons upon tons of pollutants dumped into the atmosphere, and will foul it; there will be such an enormous consumption of petroleum products that there will be a crisis of supply. Imagine trying to establish that line of argument in the 1930's; no one could have mounted the argument at that time and been successful at it.

Privacy, fortunately, has not proceeded to the pollution stage yet. Progress on the issue, public awareness and legislative initiative has been enough so far to hold the matter in check. To me, the essential thing is to get the job done, and to get all the safeguards and laws in place so we do not have an enormously difficult job to undo retroactively. Let us get the job done while it is feasible to do it. When I try to persuade you that the privacy problem is real, in part I am projecting trends in recordkeeping as well as reacting to its present status. There is a real problem, in part latent; if it gets too big, we may not be able to handle it.

Often, organizations and democracies have a way of responding only when things get to the crisis stage. To me, there are ample signals that the privacy matter is escalating at such a rate that, in my judgment, we have five or so years to get safeguards in place or else we as a country will have a massive task of retrofitting record systems.

In responding to privacy in your role as a data processing professional, I would take the position unequivocably that it is not your obligation to fix the problem; rather, it is a corporate matter. I would say to you forthrightly, bluntly, and vigorously, "Make sure that it stays that way; make sure that your management does not abdicate its responsibility and say casually,'Fix the corporate privacy problem, would you and don't bother me' ". That's an inappropriate response on an issue of this kind and it is too treacherous. Let me suggest why.

First of all, responding to privacy will inevitably have costs associated with it. What they are will depend in part where the particular installation happens to already be vis-a-vis security safeguards; if they are in place and adequate, the cost of privacy will probably be nominal--especially if supplemental actions can be instituted in the natural course of events over a convenient period of time. But, privacy concerns the use of information, which is a matter of corporate policy. The EDP organization does not control people who receive information from a system nor does it stipulate how they use it, either appropriately or for their own purposes or own motivations. Part of the problem is simply outside the purview of our EDP group.

Therefore, as a policy matter, the corporation has to take a stand and state the general policy. While EDP managers can participate in helping to create policy, management cannot pass its just responsibility off on the computing organization. Don't be the fall person.

Our appropriate role is obviously to participate in the decision-making process, to suggest what the nature of privacy is as it impacts recordkeeping, to help define the threats against a system vis-a-vis security, and to make estimates of the costs. The menu of safeguards properly comes from computer-informed people, who also play an educational role. In the end, I feel very strongly, however, that top

management must announce corporate policy and then properly expect the data processing organization to respond to such guidance.

To be more specific, there are various sets of people involved: the employees of an organization, the customers of an organization, or a set of individuals about whom an organization maintains records for some business purpose, e.g., credit, recipients of welfare, students. Each has to be dealt with vis-a-vis privacy.

Data processing people will inevitably become involved in the affirmative action steps to protect information, to maintain it as confidential, to control its use, and to do all other things pertinent to privacy. Data processing people will obviously be involved in the technical response, to make changes in record systems, to arrange mechanisms to permit people to see and copy records, to provide the capability to flag records or portions of them when disputed. There is a granularity problem, because parts of a record may have to be dealt with differently. To illustrate, consider the integrated corporate data base, which has payroll, medical history, professional status, employment status, future promotion opportunities for growth in the company--everything about a person in one record. Clearly, the record must be dealt with in component parts, because each user is not entitled to access the entire thing. Modern-day systems are not designed to work that way.

If there is a granularity problem, then there is also a data descriptor problem, because the software that manipulates the data base has to know its structure and how to deal with each component. If one system exchanges data with another, there is a mutual problem of how to handle descriptor data, because the recipient also must know how data is structured, so that it, too, can control dissemination properly.

In a different dimension on privacy, law may well not be specific. While legislation sometimes contains quantitative performance requirements or establishes specific details, most likely privacy law will establish social goals and general principles. As a data processing individual, one is in the position of deciding just what is really meant by some legislation and its legislative history. Such a position is alien to a computer person because, typically, he is accustomed to responding to carefully specified thought-to-be complete specifications. Responding to privacy law is a different circumstance.

There is yet another aspect that will be new to us and perhaps uncomfortable. The EDP person will have to share the liability for things that go wrong in record systems; they are, in fact, moving toward the front line of civil and criminal liability. Present privacy laws--as well as the new ones--have sanctions of one kind or another--typically, fines and jail sentences. If a computer person is part

of the problem and has created some situation for the corporation that results in liability, he's almost certain to be involved with the legal proceedings.

The Commission also took a position on the Social Security number. Accuracy of records is an aspect of fairness in recordkeeping; fairness in recordkeeping is a pivotal aspect of privacy. Therefore, anything that contributes to accuracy of records is good for privacy. Unique identifiers clearly play such a role; therefore, the Social Security number should be an acceptable identifier for individuals and record systems. This is the thread of the Commission's argument. In examining the federal agencies, the Commission quickly became convinced that anyone in Washington who wants the Social Security number either has it or has the authority to get it; the Tax Reform Act extends similar authority to the states. There is no way that the country could retrogress the Social Security number to its earlier role of an account identifier. However, the Social Security number should be constrained to valid recordkeeping purposes and there ought to be some constraint on what federal agencies do with it. There is a group of four recommendations addressing the Social Security number that generally parallels the position just summarized.

The privacy issue to me is real and is not going to go away; there is an immediacy about it that has to be dealt with. As practitioners of a very central technology that makes modern-day recordkeeping possible, each of us has a very key role in seeing the issue through and in helping to solve it. The country is really seeking an appropriate balance point between each of us as individuals and all the record systems that we cannot escape dealing with. I would hope that none of you as individuals nor GUIDE as an organization would decline to help resolve the social effects that our technology has largely created.