COMPUTER PRIVACY AND COMPUTER SECURITY

Willis H. Ware

October 1974

P-5354

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

TABLE OF CONTENTS

COMPUTER PRIVACY AND COMPUTER SECURITY

The word "privacy" has many and varied implications. To some, privacy connotes the option to withdraw completely from one's social environment. To others, it is the right to be left alone and not bothered by some artifact of the environment, such as unwanted mail. Yet to others, it is the right to control intrusion into--or onto--one's personal property. Because of the diveristy of meaning, invasion of privacy can grade from clear situation of obvious harm through incidents of harassment to those of simple annoyance. The classic example is the unwanted mail received as a result of the mailing list industry. Some circumstances are clearly harmful, such as pornographic mail sent to minors. In other circumstances, repeated letters or mailings from a single organization can constitute a form of harassment, while to many the act of emptying the mailbox and sorting out stuff is even pleasurable. In the context of the information system -- be it computer based or manual -- the notion of privacy fortunately can be made more precise.

The Privacy Trade-Off

An individual provides data about himself to an information system with the expectation of receiving some right, privilege, benefit, or opportunity in return, e.g., credit, a travel reservation, an educational scholarship. So long as the information is used for the intended purpose, and simply to make the intended decision, then there is in effect a mutual defacto contract between the data subject and the data owner.

However, such information can obviously be used for purposes other than those for which it was originally given. Such secondary usage may easily result in clearly discernible harm to the individual, e.g., loss of reputation, loss of job, embarrassment, public ridicule. It can also be used in a secondary way which does not harm the individual but which, if it were known to him, would be regarded as undesirable.

In the computer context, privacy has to do with protecting the individual citizen against harm which occurs as a result of the operation of a personal data system containing information about him. In a broader sense, privacy

also relates to the loss of control that the individual incurs after he has provided personal information to some system. The goal of so-called "computer-privacy" legislation is to better balance the situation between each citizen and the totality of information systems that surround him and control his life.

Technical vs. Legal Problems

In order to assure that information about an individual is used properly, an obvious early step is to make certain that an information system delivers output only to users authorized to have it for a stated purpose; usually the purpose is with regard to performing some job. In the context of computer-based systems, the matter of access control is an essential part of a larger issue referred to as computer security which can be defined as:

> The protection of the equipment, facilities and data of an information system against deliberate or accidental damage, and against denial of use by legitimate users, together with the assurance that information will be delivered by the system only to individuals authorized to receive it.

Computer security is largely a technical and administrative matter, whereas privacy is largely a legal matter.

The broad principles of protection surprisingly are generally rather well agreed on. In order to give the individual some measure of control, one finds suggestions that data banks must give public notice of operation, must establish a contact point for complaints and questions, and must keep proper access records of who uses the data. To give the individual a legal position form which to seek redress in case of harm, one finds suggestions for incorporating both criminal and civil penalties for infractions of rules. The pivotal issue at this point is how to cast such broad principles into an appropriate legislative framework.

Legislating the Issue

One possibility is a broad omnibus bill that would stipulate desired principles of good behavior for information systems and create penalties for intractions; a Federal Privacy Board would enforce the law. Another possibility is specific legislation that addresses an identified industry or group of organizations that are considered to be causing harm; the Fair Credit Reporting Act is one such example. A third suggestion is the creation of a Fair

Information Practices Code that would define the desired behavior of information systems in a very broad way and provide for criminal and civil sanctions to be invoked by the individual in case of harm.

There are, however, other important dimensions to the problem. Does the approach selected apply to the public sector or government only, and if so, to what levels of government -- Federal? State? Local? Should the selected approach apply as well to the private sector of industry, commerce and education. Or, should the approach be applied to both? Or should there be a different approach for each? Another significant dimension is the deceptively simple issue of who is in charge. Are the provisions of the law enforced by a regulatory agency that holds hearings, licenses, policies and sets rules? Or, is the judicial system of the country effectively put in charge by requiring the harmed individual to initiate legal suit for redress?

A third, and equally important, dimension is the problem of defining what "harm" is. An attractive attribute of the specific-legislation approach is that harm can be defined very precisely. In the Fair Credit Reporting Act, for example, harm is effectively defined to be denial of employment, denial of insurance or denial of credit.

Intermingled with this set of issues is the Social Security Number (SSN) in its role as an ad hoc personal universal identifier. For the American culture, the concept of a lifetime numeric individual identifier would be a significant change in behavior. While the matter of simply having or not having a number for each person may seem superficial, behind it is the very real concern that extensive data combination can readily be accomplished by linking files once personal identity is certain. For example, if a given individual is labeled by his Social Security Number in a variety of files, there is no problem of combining all information about him and thus arriving at a more complete picture of the individual than he may have ever intended to permit; so to speak, the "dossier society" becomes a reality.

A Limit to Laws

In my personal consideration of the issue, since the completion and publication of the now wellknown HEW Committee Report - Records, Computers, and the Rights of Citizens - my position has changed a number of times. What seemed at first to be a very clear-cut and straighforward solution has developed

many important consequences, principally substantial costs and operational implications. At this time, my conviction is that a broad-gauge omnibus bill should apply only to the public sector. However, it should also provide for a general principle of "data liability" whereby every individual would be held responsible for harm that he might cause by misuse or abuse of personal information. The concept is analogous to the liability each of us assumes when he drives an automobile.

The abuse of personal information in the private sector is not well documented at present and I would therefore propose that we treat problems in that area by specific legislation as difficulties are discovered. It might prove that a general principle of data liability would be sufficient to encourage "proper" behavior in the private sector, or it might prove necessary to create a few specific laws, or it might prove that so many categories of abuse appear that an omnibus approach should subsequently be enacted for the private sector. We simply cannot tell at this time and it could be a serious disadvantage to commerce, industry, and educational institutions of this country to force expensive modifications of information systems to deal with a problem whose magnitude is unknown.

Finally, one wonders what the right position on the Social Security Number can possibly be. It is, without a doubt, widely used as an ad hoc personal identifier. To outlaw its use - other than as mandated by Federal Law - would impose substantial financial burdens on many organizations, both private and public. It is obvious that it cannot be outlawed completely, yet it is equally clear that something should be done to discourage its spreading role because it has shortcomings as an identifier and because the file-linkage matter needs to be controlled until privacy safeguards are in place and shown to be effective.

The most promising thought that has occurred to me is to create legislation that would, in fact, prohibit the use of the Social Security Number as a personal identifier, except as provided by Federal law, but would also provide a mechanism whereby an organization could publicly make a case for being granted an exception to the foregoing prohibition. Such an approach would have several advantages. It would discourage the casual use of the SSN; it would provide a mechanism for the serious user of it to state his case and be publicly judged; it would provide for the first time a comprehensive picture of how personal identifiers are

being used, of the role that a personal identifier plays in the information exchange in the country, and of the necessity for, or against, one. We would, from such an approach, assemble a very important data base on which to subsequently consider the issue (unavoidable in my mind) of: "Should the United States institute a system of personal unique lifetime identifiers?"

These are the issues as I see them. At this juncture we need public exposure and public discussion of them. We as a country need to establish our position on the issue of personal privacy as it relates to the individual vs. information systems. We as a country need to create whatever legislation is needed to put the individual in an equitable posture vis-à-vis the way in which personal information about him is collected, assembled, distributed, exploited and used.

Printed in Bulletin of the American Society For Information Science
Vol. 1, No. 3, October 1974