1977

Privacy issue where do we stand?

Donald R. Wood

THE PRIVACY ISSUE: WHERE DO WE STAND?

by DONALD R. WOOD/Partner, Chicago

A serious question faces our society today: can it guarantee each citizen's constitutional right to privacy, given the magnitude of information that is routinely collected in the files of both government and business?

In the public's mind, this concern is linked to a developing technology that enables one's personal history to be flashed on a screen at the touch of a button.

What is the role of the computer in this issue of information privacy? Are the public's concerns valid?

Traditionally, such fear has centered on the federal government and information that a citizen has no choice but to provide: tax returns, census forms, medical records, welfare and unemployment applications, and so on. But it is being compounded by recent headlines:

- The Internal Revenue Service is planning a billion-dollar tax administration system that by 1985 will enable authorized employees to obtain access through 8,300 terminals to tax returns of any U.S. citizen within seconds.
- By 1979, the Social Security Administration and the Internal Revenue Service will be required by law to share incoming tax data on all W-2 forms; it is anticipated that this computerized information pool will contain more information on individual citizens than has ever been possessed by any single federal agency.

In the past decade, moreover, private organizations have developed their own information systems that can influence an individual's life to a degree that only the government could achieve in the past. Thus, given past breaches of confidentiality in regard to medical records, legislative concern arose recently with news that several insurance companies and private hospitals would have access by computer terminals to the Social Security Administration's data and response system. And given its sensitivity to credit information, more concern was prompted by news that banks would soon be linked with the Federal Reserve Board's electronic funds transfer (EFT) system.

As a result of such headlines, executive and legislative bodies on both the federal and state levels have proposed various methods to control the availability of private information to external users. And given that these concerns have arisen under a conservative federal administration, they are not likely to disappear under a more liberal administration.

What has been this governmental response? To some it has been excessive, to others reasoned.

- The Federal Information Privacy Act of 1974 was passed, stating the rights of individuals and establishing regulations governing the collection and use of information by federal agencies. Implementation began in 1976, and the results thus far are inconclusive.
- An omnibus bill, HR 1984—the Orwellian title is deliberate—was sponsored by congressmen Edward Koch (D-New York) and Barry Goldwater, Jr. (R-California). Essentially, their bill would extend the Privacy Act of 1974 to cover the information in private sector data systems. Strongly criticized by business, its fate is hard to predict at this writing, given the shifting political moods of a new congress.
- The U.S. Privacy Protection Study Commission—established by the Privacy Act of 1974—is scheduled to deliver its report to the president and congress in July. At this writing, it is expected to recommend regulations and guidelines that will protect the privacy of individuals and yet recognize the need of government and business for accurate information. Its recommendations will propose not omnibus legislation, but regulations directed toward specific industries.

In addition, more than 30 state legislatures are actively considering some type of privacy bill. (Abroad, West Germany and Sweden have already enacted privacy laws, and a privacy policy is in an advanced state of preparation in nine Common Market nations.)

Finally, the Domestic Council on the Right to Privacy, a presidential advisory group, recently called for a coordinated national information policy. It cited how the use of increasingly complex technology in the business and economic worlds has impacted the individual's ability to control information about himself.

Are computers across this nation waiting for a signal to print confidential data on anyone who has a Social Security number, an employment record, or a credit card? That appears to be the public understanding, even though little such information has yet been entered into computer systems by either large companies or small. In other words, the confidentiality that has been breached to date has primarily been through manual rather than computer transgressions.

Such facts, however, have not hampered the speculation by proponents of a privacy law. The Office of Technology Assessment, an arm of congress, tries to anticipate the implications of major new scientific developments. It has concluded that the IRS tax administrative system could pose "a threat to the civil liberties, privacy, and due process of taxpayers" and ultimately bring "surveillance, harassment, or political manipulation of files." (One sees here the influence of Watergate.)

Representatives John Moss (D-California) and Charles Rose (D-North Carolina) have suggested that the IRS be denied funds for its new system, because it would probably result in "some kind of hookup between IRS computers

and banks around the nation to check daily balances of businesses and individuals [in order to] speed collection of tax revenues and discover delinquent taxpayers."

This, of course, is speculation. It is obviously the opinion of those who have little trust in certain areas of government and the business community. But it is also the opinion of those who assume a linkage between the computer and past privacy invasions that I do not believe the facts justify.

Indeed, we need to know more about this entire subject.

—What has been the impact on government operations of the first law, the Privacy Act of 1974?

—What type of information policy is being practiced by the business community today?

—How *are* citizens' rights being affected?

—Should business practices be changed to acknowledge those rights, and if so how?

—What will be the costs of implementing such practices?

Clearly, the future effectiveness of a privacy information policy is going to depend on sincere cooperation between the business community and representatives of the general public. What both parties must agree to early is the level of risk that can be tolerated. Says Dr. Ruth M. Davis, director of the National Bureau of Standards Institute for Computer Sciences and Technology: "What we fail to recognize is that we have little skill or experience in even asking the appropriate questions to enable an adequate technology assessment" of a national computerized record-keeping network. And when those who accept the risks are not those who obtain the benefits, she has written, the problems of accountability are exacerbated.

Federal Privacy Study Due

The July report of the Privacy Protection Study Commission will likely represent the major privacy recommendations to be offered to Congress in 1977. According to advance reports, it will propose: (1) there be no secret data systems that the public is not aware of, (2) the parties concerned have access to the system, (3) the information in the systems must be accurate, and (4) that the information is confidential except when the "need to know" is clearly established.

The proposals will likely be directed toward a number of separate industries, particularly in the area of financial and health services. Self-regulation will be the key to some proposals, but specific regulations may be recommended in such sensitive areas as insurance and credit.

While the specific recommendations of the report are not known at this writing, an educated guess is possible, based on the Privacy Act of 1974 and the proposals of representatives Koch and Goldwater. They would involve unfettered access by individuals to their own records, the means to correct or amend one's own record, assurance that information be used only for the purpose for which it was collected, and obtaining all information from its source.

Supporters of such legislation claim it will make possible a consistent application of privacy legislation in both the public and private sectors. They view proposed state privacy legislation as a patchwork of overlapping and inconsistent laws that will make compliance difficult for companies having operations in more than one state. Opponents say that compliance would be difficult and expensive, severely restricting the operations of government and industry.

What is seldom discussed today is this question of practicality. An impractical law is no law at all. In addition, some of the legislation currently under discussion also raises other questions:

—Must each individual be notified whenever the system is changed, such as when a new access is requested, say based on age or weight?

—Must information be solicited directly from the source whenever "reasonably possible," rather than from separate data files that have been made for other purposes—even when it would be more efficient and accurate to collect existing file information and then confirm it with the individual?

—Must the subject be informed of the kind of source for every input into his file, as well as of every non-routine use of the data in the file?

This latter question is of interest to accountants and auditors. What is non-routine use? Let us assume that a retail store can use information on a credit application only internally as it relates to authorizing credit. Does this mean that the store's internal auditors may use the information to satisfy themselves that data security controls are adequate? Does that privilege extend to the store's external auditors?

Clearly, the future effectiveness of a privacy information policy is going to depend on sincere cooperation between the business community and representatives of the general public. What both parties must agree to early is the level of risk that can be tolerated.

Actually, if management is defined broadly, internal and external auditors should be included, since management is deeply involved in audits.

Apart from such auditing problems, of course, accounting for access could be very expensive. The cost difference is tremendous between automatic notification of every use of one's files, and providing unrestricted access to information at the subject's request.

Given the burden of such proposed legislation, is there another way for private industry to go? Indeed, a number of private enterprises have established their own meaningful privacy principles. For example, IBM's internal policy:

"(1) Individuals should have access to information about themselves in record-keeping systems. And there should be some procedure for individuals to find out how this information is being used.

"(2) There should be some way for an individual to correct or amend an inaccurate record.

"(3) An individual should be able to prevent information from being improperly disclosed or used for other than authorized purposes without his or her consent, unless required by law.

"(4) The custodian of data files containing sensitive information should take reasonable precautions to be sure that the data are reliable and not misused."

Business Sponsors Privacy Research

A more detailed response by private industry is underway at Purdue University's Krannert Graduate School of Management, West Lafayette, Indiana. An Information Privacy Research Center under director Jack Osborn is studying current practices in the business community, how they are perceived by their employees, what information needs to be stored, and how broad a company's written policy should be in regard to using information. Supporting or participating in its efforts are such organizations as Sears, Montgomery Ward, Chrysler, General Motors, IBM, Rockwell International, TRW, PPG Industries, the Data Processing Management Association, and Touche Ross. (The writer, indeed, is on the center's board of directors.)

To provide both businessmen and legislators with objective information, a number of studies are being undertaken. One will examine leading corporations in retailing and manufacturing to learn what information is actually being stored, who knows what the information consists of, why it is being stored, and how it is being used. A study by Howard Fromkin will ask employees what information they think is in their company's files, is their company justified in filing that information, and does its existence cause them any concern; the same questions will be asked of people in data processing.

According to director Osborn, the latter study may be the most extensive ever done in the field, involving 400 to 900 employees per company, with many of the companies on the Fortune 100 list. "What we are finding is that employees make a very clear distinction between the uses of information in business practices and how comfortable or uncomfortable they may be about the handling and use of that information. Employees may say that, although it does make them uneasy, it is proper for companies to use information about their health, for instance, in making decisions or promotions within the company. Legislators, however, put their finger on the 'uneasy' part and do not seem to be aware that employees do, in fact, feel that it is proper for the company to use that information."

Supporters of [federal] legislation . . . view proposed state privacy legislation as a patchwork of overlapping and inconsistent laws that will make compliance difficult for companies having operations in more than one state. Opponents say that compliance would be difficult and expensive, severely restricting the operations of government and industry.

Research must be done particularly in the area of risks. Certain informational risks are evident, but what is their frequency? And what is the cost of managing systems procedures to control those risks? Also, should government regulate in some areas and not in others? And should privacy invasions be administered by the courts on an exception basis?

Behind this research lies the knowledge of the business community that the Domestic Council on the Right to Privacy, the presidential advisory group, has called for a coordinated national information policy. The only question, it says, is whether or not the government will take this step. Will there, in other words, be an Information Protection Agency (IPA), similar to the Environmental Protection Agency in concept and scope, that might:

—develop a national policy covering the collection, dissemination, review, and security of information;
—introduce legislation encompassing both the public and private sectors;
—monitor new technology and evaluate future exposures;
—monitor proposed systems to ensure the inclusion of information protection procedures.

It is clearly in the interest of society as well as the business community to understand beforehand the practical impli-

cations of such a program. Not the least significant is that they will cost money. Robert Goldstein of the University of British Columbia has focused his research on this problem, with the assistance of Purdue's IPRC. A computer model has been developed, he reports, that will estimate the cost of a set of privacy regulations on a computerized personal data system. The model contains descriptions of the specific operational steps that would be required to comply with privacy laws. Each requirement of the law is related to six resource categories: programming, data storage, computer processing, data transmission, manpower and capital. Most of these are broken down further, so that the actual model contains about 120 primary equations.

Conclusion number one, according to Goldstein: "The imposition of a set of requirements like those included in the U.S. Federal Privacy Act increases the annual cost of operating a PDS by 15 to 25 percent. Looked at another way, the additional privacy cost seems to range between 40 and 60 cents per data subject per year."

Conclusion number two: "There now seems to be an irreversible trend in the Western, industrialized world toward recognition of a right of personal privacy and greater control of individuals over information about them. ... Regulation will be extended relatively rapidly into the areas of law enforcement information, medical records, and other types of personal data.... Preparation for this should include the addition of privacy oriented features in all new information system designs, as well as making the government aware of any aspects of proposed legislation that would be particularly burdensome. Failure to start considering privacy considerations now will almost certainly result in their being more costly to implement later."

Realistic Approach Needed

Perhaps the final plea that a realistic attitude be taken toward both the usefulness of the computer—in the conduct of business and government affairs—and the costs of privacy should be made by Alan Westin, the Columbia University professor whose book, *Privacy and Freedom*, created such a stir in the late 1960s.

"Computers," says Westin, "are here to stay. So are large organizations and the need for data. Equally real are the social cleavages and cultural reassessments that mark our era. Our task is to see that appropriate safeguards for the individual's right to privacy, confidentiality, and due process are embedded in every major record system in the nation—particularly in those computerizing systems that promise to be the setting for the most important organizational use of information affecting individuals in the coming decades." △