AMERICAN DATA PROTECTION DILEMMAS

This report is by Robert Gellman, Chief Counsel to the Subcommittee on Government Information in the US House of Representatives, who has provided much of the know-how for Congressman Bob Wise's privacy bills in recent years (PL&B July'91 p.7, 19-23). He addresses the structural problems constraining privacy legislation in the USA. Former President George Bush appeared to favour minimalist privacy legislation (PL&B Dec '91 p.3). Is President Bill Clinton interested in a stronger regulatory approach?

The major problem with privacy policy making in the United States is the lack of permanence and continuity. Each privacy issue is addressed by different groups that assemble temporarily to deal with a current problem. For example, the two agencies funding genetic research are, by default, also responsible for genetic privacy issues. These agencies are the Department of Health and Human Services, and the Department of Energy.

Low priority

Other records on privacy are handled elsewhere or nowhere. The Department of Education is responsible for privacy of education records. The Office of Management and Budget oversees the 1974 Privacy Act. The Federal Trade Commission has responsibility for overseeing US credit reporting law. To the extent that there has been a response from the USA to international data protection concerns, that response has come from the Department of State or the Department of Commerce. Unfortunately, there is little meaningful coordination or shared expertise among these agencies. At each agency, privacy has a low priority.

No political support

Congressional efforts on privacy matters have been just as fragmented. New privacy laws of a sectoral nature pass occasionally. They are most likely to be a response to a well-publicized scandal, a specific concern of a key Congressman or Senator, the quiet work of staff members, or a rare coalition of interested parties who see something to gain in privacy legislation. The division of power within the Congress makes it difficult to raise data protection issues that cut across traditional jurisdictional lines. Efforts to establish a data protection authority at the federal level have not yet attracted sufficient political support for enactment.

Opinion polls tell us that public concern about privacy is at a very high level in the United States. But no-one has been able to marshal this general concern into support for general data protection legislation. The Bush administration showed no interest in the protection of privacy. The business community will not support even the mildest law restricting its use of personal information unless it is directly threatened or embarrassed, or unless it needs protection for its own purposes.

One result of this fragmentation is a lengthy list of federal and state laws, constitutional provisions, regulations, and common law principles relating to privacy. The list appears impressive, but the actual protections for personal data are very spotty. You need to look at what is *not* on the list as well as what is there.

These laws do not bite

In addition, for the average individual, the remedies provided by law are not meaningful. It is nice to be able to sue someone for a privacy violation. But since the cost of litigation approximates the annual income for the average American, this is not much help. Also, some privacy laws provide no effective relief even for those who can afford litigation.

Let me illustrate my point with a specific example. The Subcommittee recently held a hearing on a national change of address system operated by the U.S. Postal Service. The Postal Service collects mail forwarding orders

from individuals, puts the addresses in a computer database, and licenses two dozen companies to provide address correction services to mailers. The purpose of the system is to increase the efficiency of the mail.

Postal Service rules restricting unrelated uses of name and address information are ineffective. As a result, the name of anyone who files a change of address notice will end up on a *new movers* list that is bought, sold, and used by the direct marketing industry. New movers are good customers, and the list is highly prized by marketers.

Consumers have no control over how their change of address information is used. If you want your mail forwarded by the Postal Service, then your name and address will be licensed to the direct marketing industry. There is inadequate notice of the disclosures. There is no consumer choice. When my Subcommittee Chairman proposed allowing consumers the chance to opt-out of the licensing system, representatives of the Postal Service and of several direct marketing companies were opposed. These opponents seem only interested in their own efficiency and profits. *They place no importance on the privacy rights of individuals.*

The Disease will linger

Legislation to require an opt-out was proposed and is likely to be reintroduced in 1993. Passage is uncertain. Should the legislation pass, it will be trumpeted as another example of a privacy protection law in the United States. Yet preventing the Postal Service from selling new addresses will do nothing to limit the sale of similar information by telephone companies, cable television companies, public utilities, and others. At best, the proposed legislation will treat a symptom. The disease will linger.

The international dilemma

Principles of data protection require that personal data be maintained according to fair information practices wherever the data is used or stored. This makes data protection an international problem. The quality of the privacy laws of other countries has become a legitimate subject of inquiry.

Some say the United States privacy laws are just as good as the laws elsewhere. In some respects, this is true. Statutes and constitutional provisions provide a significant barrier against the misuse of personal information by the *federal government.* Concerns about protecting individual liberties and about limiting the powers of government date back to the earliest periods of American history. The focus of privacy debates in the 1960's and 1970's was on how the government collected, maintained and used personal information.

While not perfect, our laws restricting federal use of personal information compare favourably with laws elsewhere. However, *state government* practices are not as good. Many states disclose or sell large amounts of personal data, including drivers' license, motor vehicle data and land ownership records.

Private sector data protection

Turning to private sector record-keeping activities, we find a completely different picture. There are no general data protection laws that apply to the private sector. There are some laws providing limited protection for some types of records. But there is no general federal legislation protecting the most important records of human existence. There is no federal privacy legislation for *employment records, medical records,* or *insurance records. Bank records* have limited protection against government access, but there are few statutory restrictions on how banks can use information about customers. On the other hand, records of *movie rentals* are protected by federal statute.

There are some state laws, but their protection varies significantly. For example, those states with *insurance privacy laws* have usually based them on a model law prepared by the insurance industry. These laws generally authorize insurers to do anything they want with personal information. Only uses that are

irrelevant to insurers are restricted. More states have laws protecting *medical records*, but some provide only that medical records are "confidential." Not all such laws even provide for patients' access to records. Overall, these laws provide few meaningful protections to consumers and little guidance to record-keepers.

No marketing restrictions

In my view, the major privacy problems we face in the United States involve private sector data practices. The use of personal information for marketing is accelerating. Supermarkets in the USA are now using computers to compile data on the purchases of consumers. There is evidence that some doctors and pharmacists disclose or even sell *personally identifiable information on prescription drug usage* for marketing purposes. Some hospitals may be using medical records to market services to patients. Height and weight data from state drivers' license records are used by private companies to identify potential customers for clothing in large or small sizes. State property records are routinely collected and made available by private companies through computer networks that enable anyone to find the addresses of home owners and the value of their property. Private boat and airplane ownership records are combined with publicly filed stock market transactions by companies who identify millionaires for fund raising by universities.

If you would like to see a real list that reflects American data protection practices, obtain a copy of a mailing list catalogue from an American mailing list broker. The number of mailing lists available in the United States is nearly endless. If someone compiles a list of individuals with specific genetic characteristics, it too may be used to fuel the American direct marketing industry. There are few, if any, restrictions on the collection, maintenance, disclosure and use of personally identifiable information for marketing purposes. There is no requirement to notify record subjects, no need to seek approval, no right to object, no right of access.

Unrestricted use of data defies evaluation

As a result, in the not too distant future, consumers in the United States face the prospect that a computer somewhere will compile a record about everything they purchase, every place they go, and everything they do. The airlines have information about our whereabouts and activities. Travel agents and credit card companies may have the same data. *In America this information can be sold and used without notice or restriction.*

This illustrates the problem for those who seek to judge the adequacy of American privacy laws. How do you evaluate data protection in a country where laws and policies vary considerably from state to state, from agency to agency, from company to company and from office to office? Some record keepers follow fair information practices; many do not. How do you evaluate data protection when most private uses of personal data are unrestricted?

Even if laws or policies appear adequate on their face, how can you tell if record keepers are actually complying with them? If there are industry privacy codes, they are typically self-serving documents that protect business interests rather than consumer rights. Those who prepare and subscribe to industry codes may not even be complying with them.

One of the many lessons I have learned from Professor Flaherty* is that compliance audits are an essential component of data protection. How can compliance be determined from afar? In America, we know little about the actual practices of our companies. For example, we only recently learned about longstanding conspiracies involving federal employees and private investigators who trafficked in highly protected social security and criminal history records.

Minimal oversight by federal agencies

There is little comfort to be taken from past government activities. Oversight of the federal Privacy Act of 1974 by the Office of Management and Budget continues to be minimal. In the early 1980's, the National

Telecommunications and Information Administration of the Department of Commerce undertook a major effort to secure domestic corporate compliance with the international privacy standards of the OECD. But the Director of NTIA's OECD Privacy Guidelines Project later testified that the focus was on avoiding embarrassment. As soon as the international pressure was off, the staff was no longer allowed to discuss the guidelines project with the press or to make speeches urging corporations to comply with the guidelines. Advisory functions on data privacy policies were disbanded by the fall of 1982.

Conclusions

At this still early stage of international data protection coordination, it is an exceedingly difficult task to evaluate the adequacy of privacy laws in a country that does not have a comprehensive data protection policy. In my view, adequate laws without effective implementation are useless. And because reasonable data protection practices may be found and encouraged in the absence of adequate laws, I believe that any review must give substantial weight to how a particular company or agency manages its own records.

In brief, everyone affected by international data protection rules should be offered incentives to move in a direction that will minimize economic disruptions, maximize privacy protections, and allow everyone to conduct his or her responsibilities more effectively.

* "The conduct of audits is one of the most important and least developed aspects of controlling surveillance." Professor David H. Flaherty *Protecting Privacy in Surveillance Societies* p.400 (1989) - see PL&B December '89 p.29

This is an edited version of the paper delivered by Robert Gellman, Chief Counsel to the US House of Representatives' Subcommittee on Government Information, at the Data Protection and Privacy Commissioners' Conference in Sydney, Australia, in October 1992.

Privacy Laws & Business Moves to New Offices

After six and a half years, *Privacy Laws & Business* has now moved to more spacious offices where we will be able to offer you a more efficient service helped by new staff and new telecommunications equipment, computers and printers.

In addition to the continuing sterling copy editing, office management and administrative skills of Merrill Dresner and Gill Ardeman, I am delighted to welcome our two researchers:

- **Bojana Bellamy** has a law degree from the Belgrade University Law School. She specialised in EC Law and obtained a diploma in Advanced European Legal Studies from the College of Europe in Bruges, Belgium. She has also completed her Masters thesis on European Community Data Protection Law at the European University Institute in Florence, Italy.
- **Deborah Fisch Nigri** has a BSc. in Juridical and Social Sciences from the Law Faculty of the Federal University of Rio de Janeiro, Brazil and has been admitted to the Law Society of Rio de Janeiro. In March this year, she successfully completed her doctoral thesis on computer crime at the Commercial Law department of Queen Mary and Westfield College, the University of London.

Our new address is: Roxeth House, Shaftesbury Avenue, Harrow, Middlesex, HA2 0PZ, United Kingdom. Our new numbers are: Telephone: 081 423 1300 Fax: 081 423 4536.

Stewart Dresner, Director, Privacy Laws & Business