THE CASE FOR A DATA PROTECTION ACT IN THE USA

The EC data protection draft directive has created a flurry of interest among those in the USA in business, consumers and civil liberties groups and government concerned with privacy. Member of the US House of Representatives Bob Wise introduced his bill, the Data Protection Act of 1991 (H.R. 685) 137 Congressional Record H755 on January 29, 1991 with the following statement which refers clearly to the need for the USA to respond to the EC challenge. Hearings on the bill are scheduled for September.

Mr Speaker, I am today introducing the Data Protection Act of 1991. This bill would establish a federal Data Protection Board as a permanent, independent, and non-regulatory federal agency. The legislation is virtually identical to H.R. 3669 which I introduced in the last Congress.

There are two principal reasons why data protection legislation is needed in the United States. First, Americans are greatly concerned about threats to their personal privacy resulting from the increased use of computers to collect, maintain, and manipulate personal information. Seven of ten Americans agree that consumers have lost control over how personal information about them is circulated and used by companies.

Despite the depth of these concerns, there is no agency in the federal government with the responsibility to consider the privacy consequences of modern life. We have agencies that address public health, consumer protection, civil rights, mine safety, battle monuments and marine mammals. But no agency is devoted to privacy.

Second, foreign data protection activities may have a direct and significant impact on American business interests. Many other countries have passed data protection laws and created governmental institutions with responsibilities to implement and enforce national data protection standards. Nervousness about the transborder flow of personal information has led to the preparation of a draft European Community directive on the protection of individuals in relation to the procesing of personal data. Adoption of this directive could make it expensive or impossible for American companies that need to transfer personal data to and from Europe to do business. The result could be a loss of jobs, profits, and business opportunities for America.

I would like to elaborate on each of these reasons.

Concerns about privacy

Interest in privacy is not new in the United States. One of the most enduring American values is the right to privacy. From colonial times to the present, Americans have sought the right to be left alone and have worried about intrusions into their personal lives, private papers and homes. The Bill of Rights contains several protections against invasions of personal privacy by the federal government.

Today, these traditional concerns about privacy are still vital. Individuals still want to be left alone. Individuals still want to be able to exercise some control over how information about them is used. In the computer age, threats to privacy come not only from the federal government but also from the many public and private institutions that maintain records about individuals. Almost four out of five Americans today agree that privacy should be added to the list of life, liberty, and the pursuit of happiness as a fundamental right in our Declaration of Independence.

The federal government is not the only threat to personal privacy. Using the power of modern computers and telecommunications, many private third party record keepers have developed the capacity to store detailed information about people's transactions, habits, movements, purchases, and activities. Personal information is routinely maintained by banks, insurance companies, hospitals, schools, credit bureaus, cable television operations, telephone companies, credit card issuers, department

stores, supermarkets, catalog merchants, marketers of all types, and others.

Some recent stories illustrate the wide range of threats to personal privacy:

A recent court case held that it was legal for the FBI to go to a photo store and order a copy of film left developing by a consumer. The photo store employee made a duplicate set of prints for the FBI without a subpoena or warrant. The case raises the possibility that the FBI can routinely get copies of film left for developing at film stores.

Car rental companies are running background checks on drivers without notice to consumers.

Travel agents, airlines, car rental companies, and others in the travel industry are fighting over ownership of information about an individual's travel plans maintained in computer reservation systems. Travellers are not aware of the extent to which the industry is trafficking in their private travel plans.

Some hospitals are using identifiable patient information to compile mailing lists for the purpose of selling services through direct mail.

In the 100th Congress, a bill was enacted to protect the privacy of video rental records. This is popularly known as the Bork bill, named for Supreme Court nominee Robert Bork whose video rental records were published in a newspaper. But while we now have some protection for video rental records, there is no similar protection for records of other consumer transactions and behavior. There are not formal legal protections for records about the purchase of books, music, computer software, mail order merchandise of all sorts, travel services, meals, film developing, and other goods and services purchased by consumers. Companies are able to compile, use, and sell this information without restriction and without notice to consumers.

In the not too distant future, consumers face the prospect that a computer somewhere will compile a record about everything they purchase, every place they go, and everything they do.

This information may be used by marketing companies to send targeted mail and to make telephone solicitations. If you buy a bag of potting soil, you may start getting seed catalogs in the mail. If you buy peanut butter, you may get coupons from jelly manufacturers. If you buy a pregnancy testing kit, you may get solicitations from diaper service companies. If you take a vacation at the beach, you may get travel brochures from resorts in the mountains. If you go to the hospital for a checkup, you may get an invitation to a diet seminar. If you take film to be developed, you might get a visit from the FBI.

I am not sure that this is a vision of the future that will make most Americans feel comfortable.

Functions of the Data Protection Board

We need to help consumers, businesses, and government develop policies and practices to distinguish between appropriate and inappropriate uses of personal data. That would be one of the principal functions of the Data Protection Board.

There is a reason why "data protection" rather than "privacy" is the focus of the Board's responsibility. In our complex modern world, privacy has evolved as a concept encompassing many different elements. It includes a wide range of issues about intrusive behavour, including wiretapping, surreptitious physical surveillance, and mail interception. The concept of privacy has also been cited in connection with matters as disparate as contraception and confidentiality of bank records. As the need to protect privacy has become more pressing, some aspects of its protection have become more focused. One concept that has emerged since 1970 is "data protection," which applies to the control of the collection, use, and dissemination of personal information.

The Data Protection Board that I propose would be an institutional representative for privacy issues relating to the use and misuse of personal information. The Board would be a resource, a consultant, a watchdog, and a

facilitator. The Board would not be a regulator. The Board would not be a Data Protection Registrar. European requirements for registration of personal data banks maintained by the private sector have, at best, met with mixed results. In any event, federal registration of private data banks in the United States is not a goal of my legislation.

We need a Data Protection board principally because there is no voice in government that represents and articulates data protection concerns on an ongoing basis. In the balancing of interest that shape government policies and actions, data protection needs are frequently ignored because there is no institutional spokesman to represent them. There is no existing organization that accumulates knowledge and experience in the increasingly complicated balancing of privacy interests.

A Data Protection Board could help government and industry do a better job of protecting personal information. A Data Protection Board could, with the co-operation of business, support voluntary data protection codes. A Data Protection Board could help Congress and the States shape legislation or find alternatives to legislation.

Lotus Marketplace cancelled due to privacy concerns

A very recent event underscores how a Data Protection Board might help business and consumers to address privacy concerns in a constructive way. Equifax (a credit company) and Lotus (a computer company) just announced the cancellation of *Lotus Marketplace*, a planned product that would have distributed names, addresses, and marketing information on 120 million consumers using CD-ROM disks. The product had come under heavy criticism from privacy advocates. In announcing the cancellation, the companies said that the product resulted in an "emotional firestorm of public concern about consumer privacy".

Equifax and Lotus had invested considerable sums to develop this product. This investment was lost because of high levels of consumer privacy concerns. This is where a Data Protection Board could serve a valuable role that assists both consumers and businesses. A company planning a new information product could ask the Data Protection Board to help identify and address privacy issues before risking millions of dollars that could be lost in a consumer backlash. Businesses benefit by having an opportunity to obtain an independent assessment of the potential impact of new products. Consumers benefit by having suitable privacy protections considered and included as new technologies are used. A Data Protection Board can limit the risks to all.

The need for a independent entity with responsibility for data protection policies has long been recognized. Such an organization was originally proposed during congressional consideration of the Privacy Act of 1974. The Privacy Protection Study Commission recommended in 1977 that such an entity be established to monitor and evaluate privacy laws; to continue research; to issue interpretative rules for the Privacy Act of 1974; and to provide advice to the President, the Congress, and the States. My proposal is a direct descendent of that Privacy Commission recommendation.

Most other Western industrialized nations have already established national data protection agencies. Canada established a Privacy Commissioner in 1978. Great Britain established a Data Protection Registrar in 1984. The Federal Republic of Germany (1977), Austria (1978), France (1978), Sweden (1973), Norway (1978), Isle of Man (1986), Netherlands (1988), Australia (1988) and Ireland (1988) also have permanent data protection agencies. Many other countries have passed data protection legislation in the last few years.

EC data protection draft directive

This brings me back to the second set of reasons supporting the creation of a Data Protection Board. Data Protection agencies have been established elsewhere in the world because people everywhere are concerned about how personal information is being used. By

1993, all nations of the European Community are expected to adopt data protection laws. These laws will be supplemented by a European Community Directive that will establish more uniform policies for data protection. Uniformity is viewed as essential to the completion of an internal European market that permits the unrestricted transfer of personal information throughout the European Community.

The proposed Directive concerning data protection will establish an equivalent, high level of protection in all European Community member states. This will serve to remove obstacles to data exchanges that are necessary for a internal market to function. Among other things, the Directive calls for strict controls over the private use of personal information; restrictions on transfer of personal information to third parties; informed consent as a required element of data collection; rights of access for data subjects; sectoral codes of practice for industries; and the establishment of data protection authority in each Member state.

The Directive will also have a direct effect on the transfer of personal information to - and perhaps from - the United States. The currrent draft provides:

- that personal data can only be transferred to a third party country if that country guarantees an adequate level of protection for the data;
- for notice to and involvement by the European Commission when personal data is transferred to third party countries that do not have adequate protection;
- for exceptions to the strict limitations on export of personal data only after all members of the European Community have been given the opportunity to object.

EC directive's impact on US business

American companies will be directly affected by European data protection rules in several ways:

1 American subsidiaries operating in Europe will be directly subject to the same strict data protection rules that apply to European businesses.

2 Corporations in the United States may be required to comply with European Data Protection standards as a condition of being permitted to transfer personal data from their European subsidiaries.

3 Any American company that needs personal data from a source in Europe may be subject to the European requirements for transborder data flow.

American companies that could be affected include banks, insurance companies, credit grantors, computer service bureaus, direct marketers, pharmaceutical companies, and manufacturers. Any company whose business involves the transfer of any type of personal data could become subject to European regulation. Even the simple transfer of internal personnel records from a subsidiary to an American parent company would be regulated.

The United States must prepare for the implementation of the new European data protection rules. Otherwise, American companies face the prospect of having their domestic records management practices reviewed by European bureaucrats and their legal liabilities determined by European courts. As an alternative to a regulatory apparatus controlled in Brussels, we need to formalize the American system of data protection. This could be done through a combination of new industry codes, existing legislation, and participation by a non-regulatory Data Protection Board.

I do not believe that there can be any doubt that the Europeans are serious about data protection. Some restrictions have already been imposed. Recently, the French Data Protection Commission prevented Fiat in France from transferring information about its employees to Fiat in Italy because Italy has yet to adopt a data protection law. There are rumors that some limitations on the transfer of personal information to the Unitied States may be imposed soon.

I want everyone to understand that the European Community Data Protection Directive is still a draft. Parts of it are unclear, and other parts may be unreasonable or unworkable. We do not know what the final directive will look like or how strong it will be. It seems certain, however, that there will be a directive and that it will have some impact on American business operations.

Better US privacy representation needed

Further, it remains uncertain how the American system of privacy regulation will be viewed under the new European standards. Many of the modern principles of privacy now being implemented in Europe were actually developed in the United States twenty years ago. These principles have been implemented here in a uniquely American way. The American system is hard to compare directly to more recent data protection laws because we rely on a combination of federal, state, and local legislation; constitutional protections; and common law. Some of our privacy protections surpass anything found elsewhere in the world. In other areas, the American approach to privacy protection is less formalistic and less bureaucratic than the European approach, but not necessarilty less effective. A Data Protection Board could bring a clear message about the American system directly to Europe in a creditable way.

At the very least, the United States government needs to do a better job in representing American business interests. This is an immediate need. To date, the federal governments response to data protection activities in Europe has been almost non-existent. For example, there has been no official American representative at the annual meetings of Data Protection Commissioners.

Only the Office of Consumer Affairs has paid much attention to data protection. As welcome as that attention has been, I am not sure that the Office of Consumer Affairs is the best federal representative for complex international matters with serious implications for the American business, trade, and economic interests. The State Department, Commerce Department, and United States Trade Representative should be more actively representing American interests.

While I hope that these agencies will become more active soon, it is apparent that the lack of a central data protection authority in the United States has left American industry unrepresented when decisions are made about how multinational companies can use data for transborder purposes. At the very least, we need an American federal agency to represent American interest in ongoing consultations with other national data protection agencies. The historical record demonstrates that data protection will not receive sufficient attention at any existing agency. The lack of an independent data protection authority also leaves American consumers without a spokesman for their fears about privacy.

Data Protection Board - The right response

A Data Protection Board is the right response to both domestic privacy concerns and international data protection threats to American business. The time has come to take a step that does more than respond to specific problems. We need to look to the future. We need to learn how to identify problems presented by new technology and new business methods before it is too late to react. We need to work together with record keepers and with record subjects to find ways to protect legitimate data protection concerns while allowing government and industry to function.

Bob Wise is Chairman of the Government Information Justice and Agriculture Sub-Committee, Government Operations Committee, US House of Representatives. This statement was sent to *Privacy Laws & Business* by Robert Gellman, Chief Counsel to the Sub-committee.