Privacy protection and transborder data flows

by REIN TURN
California State University, Northridge
Northridge, California

INTRODUCTION

In the last decade there has been a dramatic increase in the growth of internationally operated computer-communication systems. In these systems, in essentially a single continuous operation, data are transmitted from terminals to computers in networks that may span several countries or several continents, the requested processing is performed, and results are returned. In other cases, data files are maintained online in international, remotely accessible networks. These networks are operated by vendors of remote computing and/or information services, industry associations, or private corporations (especially the so-called multinational corporations). Some of the data transmitted in these systems are personal data about individuals.

The world-wide availability of computer-communication and remote computing services has created a "trade" in these services, complete with competition between domestic and foreign vendors, taxes and duties, and regulations that appear to prefer domestic services. However, to date the data flows have been unbalanced. Raw data are flowing to very few highly industrialized countries where most of the international data processing service vendors and headquarters of multinational corporations are located. From these countries the processed data flow back to the originating countries. Many of the latter are the industrially less developed countries in the Third World. This situation has generated considerable concern in the originating countries over their excessive dependence on foreign data processing services, and over the lack of development or loss of business of their domestic data processing industry. In general, a potential response in these countries may be to place restrictions on transborder data flows on the basis of the type and content of the data involved.

Privacy protection laws enacted in a number of European countries may provide one mechanism for restricting data flows. Privacy protection (also called "data protection" in Europe) emerged as a concern in early 1960s when automation of personal data record-keeping systems gained momentum. It was realized that automated systems are vulnerable to threats and subject to misuse on a scale that is significantly greater than in manually maintained record-keeping systems, and that individuals should be provided with certain privacy rights—legally enforceable protection against unfair practices in collection, storage, processing, use, and dissemination of personal data about them. Beginning in early 1970s the United States, Canada, and seven European countries have enacted a variety of privacy protection laws, and draft international agreements have been formulated. These laws and agreements, and their impacts on transborder data flows, are discussed in the following sections.

NATIONAL PRIVACY LAWS

Despite the differing perceptions of the problems and differing political and legal systems and traditions, the enacted privacy laws tend to grant individuals a remarkably similar set of privacy rights. A principal reason for this is that, from the beginning, privacy protection studies, discussions, debates and draft laws became widely known internationally. Thus, as the various countries tackled the problem and developed new concepts, others paid close attention and attempted to adopt these in ways that reflected their own situations. For example, the early developments (in 1969) in the Land Hessen of the Federal Republic of Germany, the studies in Canada and in United Kingdom, and the Swedish Data Act of 1973 were widely studied.

Subsequently, a Code of Fair Information Practices was formulated in the United States and international agreements on basic principles were reached in Council of Europe. Later the Code was refined and expanded by the U.S. Privacy Protection Study Commission and the international efforts in Europe to include the following principles that are applicable to both the public sector (government) and the private sector’s business, industry, and other organizations:

- **Openness**—there must be no personal data record-keeping systems whose very existence is secret, and there must be a policy of openness about any organization’s record-keeping policies, practices, and systems.
- **Individual access**—there must be a way for individuals to find out what personal data about them are on record and how they are used, and to examine those data.
• **Individual participation**—there must be a way for individuals to correct or amend records of personal data about themselves.

• **Collection limitation**—there must be limits on the types of personal data that organizations may collect about individuals, and restrictions on the manner in which they collect these data.

• **Use limitation**—there must be a way for individuals to prevent personal data about themselves collected for one purpose from being used for other purposes without their knowledge or consent.

• **Disclosure limitation**—there must be limits on external disclosures of information about individuals which record-keeping organizations may make, and there must be legally enforceable confidentiality obligations of record-keeping organizations with respect to the use and disclosure of personal data.

• **Information management**—any record-keeping organization creating, maintaining, using or disseminating records of identifiable personal data must implement data management policies and practices which assure that the collection, maintenance, use, and dissemination of these data is necessary and lawful, that the data themselves are current and accurate, and that precautions are taken to prevent their misuse.

• **Accountability**—record-keeping organizations must be accountable for their personal data record-keeping policies, practices, and systems.

There are other dimensions of privacy protection, however, where there are considerable differences in national laws, especially between those in Europe and in the United States. Important dimensions are: the scope of applicability and coverage (government, private sector, both, or certain subsections of either); data subjects covered (individuals, legal persons, or both); types of systems covered (automated, manual, or both); and types of enforcement authorities and mechanisms. These aspects of the present privacy protection laws are briefly summarized below:

• **United States.** In the public sector, the Privacy Act of 1974 covers the automated and manual systems operated by the federal government, and protects the privacy of citizens and aliens admitted for permanent residence. Enforcement is through self-compliance and courts. The Office of Management and Budget has an oversight role. At states’ level, privacy laws have been enacted in twelve states. They apply to automated and manual record-keeping systems in the public and private sectors. All residents are protected. Law is enforced by the Data Surveillance Authority. Permission is required for transborder transfers of personal data.

• **France.** The Act on Data Processing, Data Files and Individual Liberties (1978) covers automated systems and certain manual files in the public and private sectors. All residents are protected. Law is enforced by the Data Surveillance Service. Permission is required for transborder transfers of personal data.

• **Norway.** The Act Relating to Personal Data Registers (1978) covers automated systems in both the public and the private sectors. Protection is provided to individuals, and to associations or foundations. The law is enforced by the Data Surveillance Service. Permission is required for transmission of personal data abroad.

• **Denmark.** The Public Authorities' Registers Act (1978) covers government agencies that maintain automated records on residents. It is enforced by the Data Surveillance Authority. License is required for TDF. In the private sector, the Private Registers Etc. Act (1978) applies to automated systems in the private sector and protects individuals and institutions, associations and business enterprises. It is enforced by the Data Surveillance Authority. No TDF provisions are made in this law.

• **Austria.** The Federal Act on the Protection of Personal...
Data (1978) covers automated record-keeping systems in both public and private sectors. It protects individuals and legal persons or associations. Enforced by Data Protection Commission and Council. TDF provisions include a requirement to obtain permission to export data, and to process data on foreign persons in Austria.

- **Luxembourg.** The Law Governing the Use of Name-Linked Data in Data Processing (1978) covers automated systems in public and private sectors, and protects individuals and legal persons. It is enforced by existing governmental authorities. In TDF situations, if the data access point is in Luxembourg, the law applies.

In addition, privacy protection laws are pending in Belgium, the Netherlands, and Portugal. Privacy protection requirements have been incorporated in the constitutions in Austria, Belgium, Portugal, and Spain. Still other countries are in study phases that are expected to produce privacy protection legislation in the near future (e.g., Finland, Japan, Switzerland, and United Kingdom). It is important to note the tendency in the more recent national privacy laws (Norway, Denmark, Austria, and Luxembourg) to extend privacy protection to legal persons. That is, corporations, associations, and other organizations are granted the same rights regarding data about them as are given to individuals. Implications of these extensions are far-reaching. For example, if transborder data flows were restricted under privacy protection provisions of national laws, much greater proportion of data flows would be covered if legal persons were included.

### INTERNATIONAL HARMONIZATION

The similarities and the differences among national privacy protection laws can become important practical matters to governments and organizations in the private sector when transborder data flows are being considered. On one hand there is the problem of comparisons of various features in national laws in order to determine which laws are "stronger," on the other hand there is the problem to participants in transborder data flows of complying with different implementations of the same requirements. Thus, there is a general agreement that it is desirable to standardize and "harmonize" the basic privacy protection provisions in the laws of various communities of nations. In response to this, two organizations in Europe have produced draft documents—the Council of Europe (located in Strasbourg, France) and the Organization of Economic Cooperation and Development (located in Paris, France). The former is an organization of 21 Western European countries. OECD also includes non-European countries, such as the United States, Japan, Canada, Australia, and New Zealand.

The Council of Europe has drafted a Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in order to establish the following:

- A minimum set of privacy protection principles and rights to be adopted by all signatory countries (countries that are not members of the Council of Europe will be invited to join).
- Obligation of signatory countries to grant basic privacy rights to all individuals, regardless of nationality or residence.
- Cooperation and exchange of information between national data protection authorities in supervising compliance with privacy protection laws in international settings.
- Administrative mechanisms to handle disputes over jurisdiction when implementing national privacy protection requirements to handle TDF situations.

The Convention would commit the signatory countries to enact privacy protection laws based on the principles listed in the previous section. It provides a privacy protection "floor" acceptable to the signatory countries in the sense that they would consider any country that has enacted and is enforcing these principles to be providing "sufficient" privacy protection. Then personal data could be transmitted to such a country from other signatory countries without loss of basic privacy protection. The Convention is to cover automated record-keeping systems in public and private sectors. Protection is afforded to individuals, but could be extended to cover also manual systems and/or legal persons by any signatory country. However, presumably, the lack of such extensions in a signatory country’s privacy laws would not be considered a sufficient reason for restricting transborder data flows to this country by signatory countries that do have these provisions.

A parallel effort toward standardization and harmonization of privacy protection principles, rights, and requirements in the form of a set of Guidelines Governing the Protection of Transborder Data Flow of Personal Data has been completed by the OECD. The Guidelines are to be voluntary (not a legally binding treaty) on the OECD member countries that accept them, but they are regarded as "morally bound" to comply fully. The United States is expected to participate.

The OECD Guidelines are based on the philosophy that there are economic and social benefits to all participants in transborder data flows, and that it is very undesirable to establish unjustified barriers to TDF. Their purpose is to provide an interim standard until more formal treaties such as the Council of Europe’s Convention are adopted. Again, the expectation is that there would be no need to restrict personal data flows between countries that have accepted and are implementing the Guidelines’ principles and requirements. For this purpose, the Guidelines are similar to the Council of Europe’s draft Convention. That is, they are designed to be applicable to both the public and the private sectors, and to manual as well as automated systems. The protected data subjects are defined to be individuals (physical persons).
Regarding transborder data flows, the Guidelines urge the participating countries to observe the following:

- Take into account the implications on other signatory countries of domestic processing and re-export of personal data, particularly when this may result in circumvention or violation of national privacy laws of other signatory countries.
- Take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit-only data, are uninterrupted and secure.
- Refrain from restricting transborder data flows of personal data between themselves and other countries except when these do not yet substantially observe the Guidelines.
- Refrain from developing laws, policies and practices in the name of the protection of privacy and individual liberties which, by exceeding requirements for these, are inconsistent with free transborder flow of personal data.
- Insure that their procedures for TDF of personal data and for protection of individual liberties are simple and compatible with those of other signatory countries.
- Work toward development of principles, national and international, to govern the determination of applicable laws in the case of TDF of personal data.

In addition to the Guidelines which are expected to be ready for adoption relatively soon (e.g., in 1980), OECD will examine the question of restrictions on TDF of data not related to individuals, such as data on legal persons, national economy and resources, and so forth. Further, to address the non-privacy issues in TDF briefly mentioned in the Introduction, the OECD is proposing that its member countries consider adopting a “Transborder Data Flow Pledge” for a limited time period, affirming their agreement to:

- Avoid adopting national policies of restricting imports of data processing services or taking any actions to restrict TDF between the participating countries;
- Refrain from discriminating against imported data processing or telecommunications services;
- Avoid taking measures to place supplemental taxes on imported information and data processing services.
- Cooperate in setting up an international legal framework covering various aspects of TDF;
- Consult with each other on implementation of the pledge in accordance with international obligations, and taking into account the special needs of developing countries.

At this writing, none of the above international initiatives have been adopted by respective policy making bodies. There is little question, however, that they would be very useful in setting up a proper framework for handling the numerous TDF issues.

**IMPLICATIONS ON TRANSBORDER DATA FLOWS**

Businesses and industry in the United States, especially the multinational corporations and vendors of remote computing and information services, have a strong interest and dependence on unrestricted transborder data flows. Until the international agreements have been firmly and accepted by a significantly large number of countries, including the United States, the national privacy protection laws of the European countries could be used to justify placing restrictions on data flows from these countries to the United States.

Privacy protection in the context of transborder data flows deals with extending any privacy rights that individuals may have in their “home country” to any “host country” where personal data about them may be processed, stored or used. The purpose is to ensure that:

- Individuals could continue to exercise their home country privacy rights regardless of the physical location of the personal data about them.
- Record-keeping organizations in the home country could not export personal data abroad in order to evade privacy protection requirements in the home country. That is, they should not be able to establish data havens abroad, nor make use of any existing ones.
- Personal data maintained abroad would be protected from unauthorized use or dissemination by parties in the host country, and from deterioration of quality (accuracy, completeness, currency) while abroad or in transit.
- Individuals would have privacy rights vis-a-vis personal data about them collected directly in the home country by foreign organizations, or collected while they are abroad.

In general, reaching these goals requires that privacy protection laws in the host country provide protection to foreign nationals, special agreements exist to permit foreign nationals to exercise their privacy rights in host countries (e.g., the international initiatives discussed in the previous section), and contracts or licenses bind involved organizations in the host country to abide by data confidentiality, security and quality requirements. If agreements cannot be made to the satisfaction of a home country’s privacy protection authorities, these may apply the TDF clauses in their privacy laws to restrict personal data transmissions to countries that have weaker privacy protection laws.

The results of comparisons of the privacy protection afforded in the United States versus protection afforded in Europe as based strictly on privacy protection laws now in force are likely to indicate that privacy protection in the United States is less comprehensive in the following ways:

- The scope of coverage is narrower since both the public and private sectors are incompletely covered in the United States — even though the federal government is covered by the Privacy Act of 1974, only twelve states
have enacted fair information practices laws. In the private sector, only consumer credit, educational institutions, and financial institutions are covered. European privacy laws cover both sectors quite completely.

- The Privacy Act provides privacy protection explicitly only to citizens of the United States and aliens admitted for permanent residence. Thus, foreign nationals other than specified above are not covered. European privacy protection laws appear to make no distinction regarding nationality or citizenship.

- No central, independent privacy protection authority exists in the United States to enforce compliance with privacy protection laws. Under the Privacy Act, Office of Management and Budget has a nominal role of coordinating compliance, and the President makes an annual report on compliance to the Congress. Compliance with federal privacy laws that apply to the private sector is with agencies that normally regulate the areas involved (e.g., the Federal Trade Commission, the Federal Reserve System, and the Department of Education). This distributed authority contrasts with the strong, central data protection authorities in Europe.

However, comparisons of privacy protection laws are likely to give a misleading picture of the general level of privacy protection in the United States. The scope of the U.S. privacy laws is broader since they cover also manual record-keeping systems. Private sector privacy laws apply to all residents. The state fair information practices laws are only a small fraction of privacy protection activities in states. More generally, the Constitution of the United States, and those of the individual states, place strong emphasis on openness in governmental decision making processes, and establish an atmosphere of concern for individual rights. The lack of a central privacy protection authority is, itself, an illustration of the American aversion to concentrating power in government agencies. Practices such as a universal identification number for each citizen or publishing the earnings and income of all citizens, as presently exist in Sweden, would not be acceptable to Americans. Finally, to reduce the incompleteness of coverage in the private sector, bills were introduced in 1979 to establish fair information practices and place limits on use of personal information in the maintenance of medical records, financial information, insurance records, and research records.

The differences in scope of coverage of the national privacy protection laws have resulted from differing philosophies of regulation. The European countries have adopted an "omnibus" approach that applies the same set of requirements (usually with some exceptions) uniformly to the government and all parts of the private sector. In United States and Canada, where federal system of government is strongly established, based on considerable separations in powers and jurisdiction, a sectoral approach has been taken — separate laws are enacted (or existing laws are amended) to provide privacy protection in specific parts of the public and private sectors. Each approach has its merits and drawbacks. Omnibus legislation establishes uniform requirements, but cannot handle easily any specific situations. Sectoral legislation is easier to enact and permits flexibility in handling exceptions, but is likely to result in scattering of privacy protection requirements throughout the entire legal code.

In view of the above discussion, it is important for the U.S. enterprises involved in TDF and desiring to continue, to find means to convince the privacy protection authorities in the countries they operate of their commitment to privacy protection principles, and their willingness and ability to provide privacy protection at levels that match the requirements in the respective countries. The specific measures taken depend on the nature of the enterprise and its TDF activities, the nature of data involved and processing performed, any uses made of the data by the organization, and the laws in force in the home country. An effective approach appears to be the voluntary compliance and implementation of privacy protection requirements that apply to the private sector area involved (e.g., adoption of the recommendations of the U.S. Privacy Protection Study Commission that apply to the area27), as well as adoption of the principles of the OECD Guidelines.

Voluntary compliance has been urged by the Privacy Protection Study Commission, by the President of the United States at the introduction of his privacy protection initiatives in the Spring of 1979 (with special emphasis on voluntary compliance regarding employment and commercial credit granting records), and by industry and business groups, such as the Chamber of Commerce of the United States28 and the Business Roundtable.29 In addition, codes of conduct or ethics have been suggested as one avenue toward effective voluntary compliance with privacy protection principles and requirements in national as well as TDF contexts. On an industry association level, codes of conduct and effective sanctions for noncompliance could discourage organizations from using personal data contrary to privacy protection principles. On the employee level, such codes could discourage improper handling of personal data, especially the personal data on foreign nationals. However, at this time codes of conduct or ethics are not sufficiently strong to be depended upon for satisfying privacy protection requirements.

Compliance with privacy protection requirements can involve substantial changes21 in operating procedures, record-keeping systems and practices, personnel requirements and training, and substantial costs.22 Thus, there are few incentives for voluntary compliance without any other compelling reasons, such as continued participation in TDF activities. While a number of large firms have adopted voluntary privacy protection programs (usually regarding employment records) others appear to be delaying. For example, a recent survey of the top 500 corporations in the United States (with 145 respondents) showed that most of the respondents have not informed their employees of dissemination of their records to credit agencies, and over 80 percent do not allow their employees access to medical information about them used in employment-related decisions.23 Some foreign privacy protection authorities have already cited these results...
as evidence that there is little intent by U.S. enterprises to abide by voluntary guidelines proposed by OECD.

Despite the present difficulties in understanding how voluntary compliance could be achieved to satisfy privacy protection authorities in other countries that the privacy rights of their nationals will not be reduced when their personal data are in the United States, voluntary compliance is an alternative that could be implemented quickly and in ways that adapt readily to the specific requirements in any particular transborder data flow case. Efforts must be continued to develop an effective approach and implementation mechanisms.

CONCLUDING REMARKS

Transborder data flows among certain industrial countries are increasing, but most of the data processing is done in only a few countries, especially in the United States. This is viewed by countries where data flows originate as not in their national interests. At the same time, concerns over human rights have led to the enactment of privacy protection laws in numerous countries in Europe, and in the United States, with many other countries likely to follow. At the present time, the enacted or proposed privacy laws in Europe are more comprehensive than U.S. laws, and can provide a rationale for restricting transmissions of personal data to the United States. One mechanism that U.S. enterprises involved in transborder data flows can use to reduce the potential for restrictions is to adopt the OECD guidelines voluntarily until governmental or legislative initiatives in the United States have reduced the present discrepancies.

ACKNOWLEDGMENTS

This paper is based, in part, on the report by AFIPS Panel on Transborder Data Flows which the author edited as chairperson of the Panel. Major contributors to the report were panel members Roger N. Allen, George I. Davida, Eric J. Novotny, Susan H. Nycum, David M. Rappaport, Alexander D. Roth, Phillip A. Tenkoff, and Willis H. Ware.

REFERENCES


14. Privacy and Computers, Department of Communications/Department of Justice, Information Canada, Ottawa, Canada, 1972.


