Barriers to International Data Transfer

Effy Oz
Wayne State University

Free flow of information is one of the corner stones of free trade and economic growth. Communication networks now connect millions of commercial organizations throughout the world. Ostensibly, the networks could contribute immensely to the welfare of businesses, but there still exist many legal barriers that prevent genuinely free flow of data and information across borders. Strict laws in European countries forbid U.S. businesses to tap private data. This prevents free flow of information within multinational corporations and hinders marketing efforts of organizations that wish to target their products and services to selective consumers in foreign countries. The article reviews cross-border data transfer laws of different countries and the international effort to harmonize legislation.

The availability of telecommunication networks is vital to the world’s economy. Networks cover almost every country on planet earth. CSNET consists of some 200 host computers providing service to government and private research institutions in the U.S., Canada, Australia, France, Germany, Israel, Japan, Korea, Sweden and England. SWIFT (Society for Worldwide Interbank Financial Telecommunications) and CHIPS (Clearing House for Interbank Payments System) are operated by banks and credit institutions. Airline reservation systems service airlines worldwide. EURONET, in the European Economic Community, serves European countries and is connected through gateways to US and Canadian networks. TRANSAC (France), ACSNET (Australia), IPSS/PSS (England), NORDIC (Scandinavia), Junet (Japan), and VNIIPAS (the formerly Soviet Union) are connected through gateways to form one huge, meganetwork (Madsen, 1989). Bitnet, the academic network, connects thousands of universities around the world. Soon, the meganetwork will expand to millions of users in the People’s Republic of China. INTERNET has grown from an American network to a global network whose size no one knows, but it is considered the largest network.

Technically, the world’s business community can collect, maintain, and transfer data as if there were no national borders. Technically, but not legally. In an age when information is so important for the development of new markets, many countries restrict the free flow of information between their territory and other countries. Some countries forbid the transfer of classified data to other countries. They rationalize that information is wealth as is cash and tangible assets. Information has the power to give one country a political and technological advantage over another and, as a result, threaten a nation’s security. It is legitimate for a government to prohibit foreign access to research and development data, financial information, and other information that may jeopardize economic, political, or cultural interests, or even compromise the nation’s sovereignty.

Economists, however, agree that one of the most important conditions for the world’s economic growth is the free flow of information. Also, the restrictions on data transfer interfere with the smooth running of multinational companies. The number of these companies is growing. For these companies, restrictions on international data flow amount to not less than a restriction of data transfer from one department to another.
The purpose of this article is to review the current status of cross-border data transfer laws, the impact of the laws on international business, and the effort of international organizations to harmonize the laws and reach an international agreement.

**Literature Review**

Crossborder data transfer has been predominantly the concern of the legal and business communities. As the technical issue has been resolved, recent literature addresses other, non-technical issues. Authors expressed several concerns of government: economic changes and shifts in balance of payment, preservation of sovereignty, undesired political influence, cultural imperialism, compromise of national security, and privacy. All, or some of these concerns are discussed in virtually every book and article on transborder data transfer (Basche, 1983; Butler, 1983; Chandran, Phatak, and Sambharaya, 1987; Coombe, 1983; Deans and Kane, 1992; Greguras, 1980; Oz, 1994; Sauvant, 1984; Tsanacas, 1985).

While many of the problems have been resolved through negotiation and mutual agreement sponsored by the United Nations and other international organizations, one still remains unresolved: privacy. Interestingly, despite the importance we attach to privacy, the value is not even mentioned in the constitutions of the US and many other countries. Yet, a majority of the democratic nations try to protect privacy.

National governments have different approaches to the issue, as is reflected in their laws. Some are willing to forego some privacy for the sake of freer flow of information and better marketing. Others restrict any collection of private data without the consent of the individual. Thus, recent literature on transborder data transfer is intertwined with discussion of privacy (Deans and Kane, 1992; Oz, 1994; Tsanacas, 1990; Weinrich, 1990). The following discussion focuses on the main barrier to international flow of information: the disharmony of privacy protection laws.

**Laws Governing Data Privacy and Transborder Data Transfer**

To a large extent, laws governing cross-border data transfer stem from a nation’s approach to the privacy of its citizens and organizations. Over thirty nations have data privacy laws, and many more are considering either regulations or national legislation. Austria, Denmark, France, Germany, Norway, and Sweden enacted their laws in the 1970s. Luxemburg, England, and Holland joined in the 1980s. On other continents, Canada and New Zealand enacted privacy statutes. Almost all of the West European countries have laws that protect private data.

Data protection laws may be classified according to three criteria:

1. the sector whose data bases are protected: only the private sector, or both the private and public sectors;
2. the manner of storage of data protected: only automated, or both automated and manual storage; and
3. the legal entity that is protected: only natural persons, or both natural and legal persons, i.e. organizations.

Except for the American and Canadian acts, the laws apply to both the public and private sectors, i.e. both government and private organizations are subject to the same regulations of collection, maintenance, and disclosure of personal data. Over half the laws (including the US federal statute) encompass manual as well as computerized record-keeping systems. A minority of the laws apply to legal persons.

Countries that favor protection of data on legal persons argue that it is difficult to separate data on individuals from data regarding the business activities that are performed by the individuals. This is especially so with respect to small businesses. For example, the financial information of a small business also reflects information about the person, or a small group of people, who run the business. Also, a large corporation may unfairly compete against a smaller firm if it has access to the smaller firm’s data (Deans and Kane, 1992). Denmark, Austria, and Luxemburg are among the countries that protect the privacy of legal persons’ data.

Privacy legislation in the US has taken place predominantly at the federal level. The US Congress passed a series of laws in the 1970s and 1980s to tighten the rules of collection, maintenance, and dissemination of personal data: Fair Credit Reporting Act of 1970, Privacy Act of 1974, Right to Financial Privacy Act of 1978, Privacy Protection Act of 1980, Electronic Funds Transfer Act of 1980, Debt Collection Act of 1982. The laws require federal agencies to inform individuals the purpose of soliciting their data, how they will be used, and to whom they may be transferred. Individuals have the right to peruse their records which are held by federal agencies.

Furthermore, under the Freedom of Information Act of 1966, citizens have access to many types of information maintained by the federal government even
Related Content

Manipulating Temporal Cues and Message Concreteness for Deal Communication: A Study on Microblogging Site
www.igi-global.com/article/manipulating-temporal-cues-and-message-concreteness-for-deal-communication/246099?camid=4v1a

Development Attributes of Quality for E-Supply Chain System
www.igi-global.com/chapter/development-attributes-quality-supply-chain/4548?camid=4v1a

Global Information Technology Architectures
www.igi-global.com/article/global-information-technology-architectures/51245?camid=4v1a

What Drives Information Security Policy Violations among Banking Employees?: Insights from Neutralization and Social Exchange Theory
www.igi-global.com/article/what-drives-information-security-policy-violations-among-banking-employees/124901?camid=4v1a