MULTINATIONAL COMPUTER SYSTEMS

An Introduction to Transnational Data Flow and Data Regulation

Harry S. Katzan, Jr.

MULTINATIONAL COMPUTER SYSTEMS

An Introduction
To Transnational Data Flow
And Data Regulation

Harry Katzan, Jr.

Chairman, Computer Science Department
Pratt Institute

International Series on
Data Communications and Networks

International Series on
Data Communications and Networks

Multinational Computer Systems: An Introduction to Transnational Data
  Flow and Data Regulation, Harry Katzan, Jr.

FOREWORD

Silently and relentlessly, the technology of computers and telecommunications has been expanding, amoeba-like, moving this way and that, engulfing the information systems of society. From the relatively simple credit records of the local department store to the most complex information systems spanning continents by way of satellite, electronic technology is transforming our way of life.

Along with its advantages, the electronic information society has also brought unanticipated complications and even danger to our personal privacy, to the character and texture of our national life, and to relationships with our friends and foes around the world. These dangers stem not from any conspiracy to deprive individuals or even nations of their privacy and autonomy. Rather, because the technology of collecting, storing, retrieving, and disseminating information has developed so explosively, there has not been time for the gradual evolution of the social mores, laws, and treaties needed to deal with it.

Thus, the problem takes on major international proportions, affecting relations between those nations having preeminence in computer and telecommunications technology, and those lagging behind—both developed nations and developing nations. Canada, for instance, is concerned that the southward flow of data for servicing in the United States—because of our technical superiority—is causing a drain on its economy. Brazil is alarmed that permitting data to move in and out for processing purposes will force a dependence on foreign corporations, constituting a new form of colonialism—this time through telecommunications networks.

It has been difficult to understand the scope of this dynamic problem due to the lack of adequate literature setting forth the broad and complex ramifications of the issues. This timely work by Professor Harry Katzan, Jr., helps fill that need.

DAVID F. LINOWES

PREFACE

Among the major problems facing multinational organizations are controlling and monitoring the growth of computer facilities across national boundaries. Multinational computer systems are relatively easy to justify because of the economic factors involved, and computer decisions are frequently made without due regard to the problems inherent in the technology and in the organizational and international environment. The primary objective of *Multinational Computer Systems* is to translate the technical, political, and economic issues of multinational computer systems into a coherent and readable form accessible by executives, managers, and decisionmakers. While the issues are relevant to computer decisions, the subject matter itself should be of interest to all persons involved with international business. The contents of the book are covered in six chapters and seven appendixes. The chapters cover the following topics:

- Overview of data regulation
- Notes on liberty, freedom, and rights
- Information technology
- Personal privacy in recordkeeping systems
- Approaches and activities in data regulation and transborder data flow
- Multinational systems

The appendixes give resource documents on various aspects of the subject matter.

Multinational Computer Systems is concerned with personal privacy in recordkeeping systems and with transnational data flow as they relate to four general classes of multinational systems:

- International computer-service companies
- On-line systems of multinational organizations

- International service networks
- Distributed systems

These systems have a wide international impact, and several governments believe the regulation of transborder data flow to be a new challenge and a new obligation. Thus, this book covers the subjects of transnational data flow and data regulation from several points of view and represents technical, economic, and political factors.

The book is intended for executives, managers, and decisionmakers concerned with multinational computer systems and transborder data flow. The reader need not have a computer background to benefit from it.

It is a pleasure to acknowledge the insight and cooperation of Larry Hager, senior editor, Van Nostrand Reinhold Company, who had the foresight to publish a book on the groundbreaking subject of multinational computer systems; the contribution of Alberta Gordon in expertly managing the complex task of producing the book; and the editing of Patricia Mansfield, who greatly improved the quality of the book. My wife Margaret assisted with manuscript preparation and was an excellent partner during the entire project.

HARRY KATZAN, JR.

CONTENTS

1

OVERVIEW OF DATA REGULATION

It is a paradox, but perhaps we have to regulate the free flow in order to keep it free.

JAN FREESE*

To the layman, the widespread use of computer-based information systems must seem like a revolution, equivalent, at least in scope and magnitude, to the invention of movable type for book printing. The printed word has enabled the average person to become literate and thereby to actively participate in the dynamics of modern society. The rapid expansion of information technology, however, has made a lot of people illiterate on the subject of computers. Their natural reaction, in many instances, has been to believe that computers and computer people exist in a world of their own.

Expansion of information technology

To persons in the computer field, the task of staying abreast of a rapidly expanding technology has left little time and energy with which to be concerned with the social impact of the marriage of computer science and telecommunications. Because early data processing systems were simply mechanized versions of easily understood manual methods, the evolution of information technology to the point where vast quantities of information are everywhere available at a moment's notice has taken many computer people by complete surprise. Today's on-line information systems in no way resemble yesterday's manual procedures, and many of the people involved with them lack the conceptual foundation that would allow them to assess the societal impact of the new technology. In short, it is not a matter of knowing

Societal impact of information technology

---

* Extract from the proceedings of an Online Conferences Ltd. conference and the subsequently published *Transnational Data Regulation: The Realities* (1979).

about and understanding recent advances in computers and telecommunications—technical people are very good at that kind of thing. It is, simply stated, that we are not exactly sure of what is being done with the new technology or of where the advances being made will eventually lead us. Clearly, the end result in both cases may be the same or very similar. Like surfers in a busy ocean, society is riding a swell of computer and telecommunications technology, and we would simply like to know the direction we are heading in and where we will land.

If, in fact, the social impact of computers and telecommunications technology is now—or will become—a problem to modern society, then a feasible solution is the creation of a generation of generalists, who know both computer technology and its societal impact. They would enable us to enjoy the fruits of the information explosion and to take full advantage of the versatility of modern computers.

Erosion of personal privacy and diminution of individual liberty

Annoying dislocations invariably accompany emerging technology. For instance, one can imagine the plight of the blacksmith in the early 1900s after the widespread acceptance of the motor vehicle. However, a new type of dislocation is associated with information technology: it involves the erosion of personal privacy and the diminution of individual liberty. This is perhaps the most significant problem to be solved by our hypothetical generation of generalists, and time to assess the problem is clearly in short supply.

Reasons for regulation

We simply do not have time to wait for the development of generalists, however, and so it falls upon the shoulders of today's organizations to protect privacy and insure liberty as part of their normal recordkeeping activity. Many European countries have already passed laws governing the transborder flow of information in order to protect the domain of their citizens. Obviously, there are other reasons for regulating the flow of data, which may very well affect the manner in which many multinational companies do business.

Regulation of technology

Essentially, we are talking about regulating technology—in this case, data flow through the use of computer and telecommunications technology. Other technologies, such as various forms of transportation, have been regulated in the past and are regulated today. However, this does not automatically imply that computers must be regulated as well. In fact, such regulation may turn out to be ineffective because advanced technology may provide a means of circumventing it. Considering the pace of advances in computer and tele-

communications technology, staying one step ahead of current legislation does not provide even a small challenge.

PRINCIPLES OF REGULATION

One way of looking at regulation is as the administration of society in the interest of its citizens. As a procedural technique, regulation is customarily regarded as being developed on either an *a priori* or an *a posteriori* basis. Development on an a priori basis involves a determination of rights and activities that should be protected and the subsequent enactment of regulations that should in fact protect the specified rights and activities. In short, adverse consequences are determined on a hypothetico-deductive basis, and laws are passed with the ultimate objective of preventing the consequences from occurring. Development on an a posteriori basis involves the identification of rights and activities that have been abused, from a regulatory point of view, and the subsequent enactment of laws that would forestall the widespread occurrence of these abuses. In short, adverse conditions are determined on an empirico-inductive basis, and the ultimate effect of the conditions are predicted. Laws are then passed to prevent the consequences from occurring. **Development of regulation**

Another aspect of the situation concerns the manner in which the desired conditions are obtained. One approach involves the creation of a *controlling agency* to govern an activity that could result in undesirable consequences. Licenses are issued, and only those persons or organizations that have secured a license may engage in the activity—a driver's license, for example, would fall into this category. Thus, the controlling agency achieves enforcement by establishing requirements for obtaining a license, by handling complaints and violations, and by performing investigatory work. Both the regulations and the controlling agency are commonly established by one act; this is known as the *omnibus approach*. The use of a controlling agency is normally associated with legislation determined on an a priori basis. **Controlling agency**

A second approach is to enact laws that make certain types of activities illegal and to establish, either explicitly or implicitly, corresponding penalties for infringement. This approach, which is essentially self-enforcing, requires a minimum level of government intervention and is enforced through the *judicial process*. Inherently flexible, this ap- **Judicial approach**

proach is normally associated with legislation determined on an a posteriori basis.

KEY FACTORS IN DATA REGULATION

Data subject

One of the beneficial aspects of the present concern over data regulation is that it places the person about whom data are recorded in proper perspective. Whereas such a person may be the object in an information system, he or she is regarded as the subject in data regulation. This usage of the word *subject* is intended to imply that a person should in fact have some control over the storage of relevant information.

Beneficial user

Agency

More specifically, the *subject* is the person, natural or legal, about whom data are stored. The *beneficial user* is the organization or individual for whom processing is performed, and the *agency* is the computing system in which the processing is performed. In many cases, the beneficial user and the agency are members of the same organization. In fact, the subject, beneficial user, and agency may all be part of the same organization. In most cases, however, this will not be the case. For example, the agency may be a service company, and the subject may be a creditor.

In general, the beneficial user benefits from the data processed and has some control over the manner and time span in which the processing is performed. The agency need not be aware of the end use of the data or of how and when the processing is performed.

Questions of privacy and liberty

The heart of the issue is *data protection,* which normally refers to the protection of rights of individuals. While the concept may also apply to groups of individuals, such as organizations or nations, the individual aspect of the issue also raises questions of privacy and liberty. Clearly, *privacy* refers to the claim of persons to determine when, how, and to what extent information about them is disclosed. However, it is also important to realize that it refers to freedom from intrusion and to freedom of thought, choice, and action. Thus, the notion of privacy noticeably extends beyond the control of informational resources.

CONSIDERATIONS IN DATA REGULATION

One of the primary objectives in regulating data flow is to protect against the negative consequences of modern information technology. Thus, data regulation can be viewed as

the balancing of the freedoms and rights of the individual with the common interest of society. This process, normally interpreted as the stabilizing of information technology through the use of legal procedures, has in itself negative consequences; that is, laws and tariffs may seriously disrupt the flow of information upon which modern society is dependent. In fact, many people feel that the free international flow of information is a fundamental aspect of a comprehensive human rights program. **Stabilizing information technology**

Some countries resist the free flow of information across their borders because that information may erode their authority and control over their citizens. Others are concerned about the erosion of culture and traditional values. Still others are concerned about an increasing dependence on foreign information systems. The preceding discussion gives a flavor of the conditions that presently exist, which are covered in detail in Chapters 5 and 6. **Existing conditions**

PRACTICAL ISSUES IN DATA REGULATION

Although computers and modern information systems have not created the human rights issue, it is important to recognize that one of the basic methods of sustaining human rights is nevertheless achieved through the free flow of information. However, considerations of human rights, freedom of expression, and the invasion of privacy must be kept separate from the technical factors involved. Information technology can only provide a means of protecting privacy and promoting the unrestricted flow of information across international boundaries. **Human rights**

The substance of privacy laws effectively determines that the technical means of achieving privacy in information systems be commensurate with the level of risk involved. Thus, the level of security provided by an information system can be expected to depend upon the sensitivity of the data. Clearly, the cost of obtaining restricted data through the penetration of an information system would not exceed the value of the information. In fact, even though the data may not be sensitive, the manner in which they are used may constitute an invasion of privacy. **Cost of achieving privacy**

Practically speaking, a clear definition of what constitutes private and personal information is lacking. As a substitute for a sensitivity ordering of personal data, there is a general belief that more sensitive data are positively correlated with **Sensitive data**

the degree of seriousness of an invasion of privacy and the need for data protection. (Relatively unimportant data such as family status, employment, education, and hobbies have low sensitivity, and it is not generally regarded as serious if they are revealed. On the other hand, credit and other financial data have high sensitivity, and it is more serious if they are revealed because it may result in lawsuits, etc.)

In providing data protection in an information system environment, two controls are particularly important:

Controls for data protection

1. Measures must exist to protect against unauthorized new uses of data. (This refers to the merging of files and the exchange of files between agencies.)
2. Data protection must exist independently of the agency and its location. (This refers to files that are transferred to other jurisdictions with confidence that data-protection laws are complementary.)

Clearly, the most important aspect of controls over the use of data is whether they are enforceable; this is precisely why it is important to deal in general principles. As mentioned previously, advanced technology may provide the means of circumventing detailed regulations.

DATA VAULTS, DATA HAVENS, AND RELATED CONCEPTS

Misuse of information

As the cost of computer networks and associated data processing decreases, there is a growing concern over the misuse of information by businesses and government. Data vaults and data havens are concepts employed to prevent the misuse or even the use of information. While these notions are not of an immediate or long-range concern in data regulation, they provide important background material.

Data vault

A *data vault* is an operational situation wherein data from one country are stored and processed in another country in order to obtain special protection for the parties involved. For example, a national company may assure its clients that personal information is stored in a foreign country beyond the reach of national authorities. Such storage constitutes a data vault when its data-protection laws guard against disclosure.

A *data haven* is an operational situation wherein data from one country are stored and processed in another country