PREFACE

More than 100 years ago, long before the concept of "data" in its contemporary sense was conceived of, the French historian Alexis de Tocqueville postulated that "[i]f the private rights of an individual are violated . . . the manners of a nation" are corrupted, jeopardizing the entire society.[1]

With the advent of computerized data processing, the threats to personal privacy have multiplied in a manner undreamed of in de Tocqueville's day, and the state of technology continues to be refined at a pace far in advance of the necessarily deliberative pace of the laws passed in an attempt to deal with the problem.

This book is a mere snapshot in time of the contemporary state of some of these attempts in seventeen representative countries, mostly in Europe, but also in North America and the Asia-Pacific region. Their stories are framed in the context of an introductory chapter on the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which entered into force on 1 October 1985, and Draft Directives in the field of data protection published by the European Community (EC) Commission in November 1990.

The Impetus of International Law

The issue of privacy protection in connection with the use of data was first addressed by the Council of Europe in 1968, when the Council recommended that the Committee of Ministers examine whether existing law offered adequate protection to the right of personal privacy *vis-à-vis* modern science and technology.

As a result, by 1974, the Committee of Ministers had adopted two resolutions to establish minimum standards of privacy protection with respect to information in data banks.

With this impetus, within five years, seven Council of Europe Member States (Austria, Denmark, France, Germany, Luxembourg, Norway, and Sweden) had enacted general data protection laws, and two other Member States (Portugal and Spain) had incorporated privacy protection *vis-à-vis* data use as a fundamental right in their Constitutions.

The next step was seen to be the adoption of a convention to reinforce national rules on an international basis. Accordingly, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personnel data was approved and opened for signature on 28 January 1981.

Presently, the Convention has been signed by nineteen countries and has come into effect in Austria, Denmark, Finland, France, Germany, Iceland, Ireland, Luxembourg, Norway, Spain, Sweden, and the United Kingdom.[2]

While the purpose of the Council of Europe Convention is to secure privacy rights with regard to the automatic processing of personal data, the emphasis of the European Community has been on the freedom to provide transborder services, including transborder data services.

Within the context of the European Community, restrictions on the free flow of data are therefore severely limited; however, some restrictions may be imposed in the public interest, and, arguably, protection of privacy could constitute a public interest.

The European Parliament has been the most active EC organ in calling for protection of the individual privacy in the area of data protection. As early as 1979, it called for a Directive on the harmonization of legislation of data protection to provide Community citizens with such protection. In 1982, it adopted another resolution calling on EC Member States to ratify the Council of Europe Convention. Currently, all EC Member States have done so.[3]

A third international convention has been influential on European countries in the evolution of their legislation on privacy and data protection. The European Human Rights Convention, in Article 8, states an independent personal right of individuals to protection of their privacy with respect to data. The Austrian Data Protection Act, for example, which was signed into law in 1978, is based on Article 8.

The Uneven March toward Comprehensive Legislation

The reader will learn that some of the countries represented in this book passed comprehensive data protection legislation early (i.e., Austria, 1978); some only recently (i.e., Belgium, 1992); and that, in some, such law reform proposals are pending (i.e., Hong Kong[4]); while, in others, such legislation has been piecemeal and probably will remain so for years to come (i.e., the United States.)

That such piecemeal legislation is inadequate to deal with the problem was pointed out recently by an American commentator who wrote that, despite numerous data protection laws in effect in the United States, as a private citizen, he was nevertheless able to get detailed credit reports on former Vice President Dan Quayle and CBS newsman Dan Rather -- with a well-known television personality's home telephone number provided as a bonus by the information company that sold him the credit reports.[5] What better proof could there be of de Toqueville's postulate.

Another concern has been cited by civil liberties groups in the United States worried about the impact of a national health-care data bank, proposed by President Bill Clinton as part of his health care reform bill. They are concerned that such a data bank could be used by insurance companies and others to pry into patients' medical records. They note that existing privacy laws do a better job of shielding an individual's video-rental records than of keeping medical records private.

The groups are mounting a campaign to tighten laws protecting the confidentiality of medical records rather than calling for passage of a general data protection law.[6] This is unfortunate but may be necessary in a society where organizations holding personal information have discovered that information is a valuable commodity which can be bought and sold to produce revenue.

Data Protection Principles

Where general laws do exist, they often adhere to similar basic principles. Finland's experience can be used as an example. The committee responsible for Finnish legislation stated nine basic principles to be followed in drafting legislation:

(1) The general principle of the duty of care of the controller of the file in following the data protection law;
(2) The use and delivery of personal data only for a necessary, predefined purpose;
(3) Restrictions on the compilation of "sensitive" data (i.e., data about racial or ethnic origin; social, political, or religious convictions; criminal acts, punishments, or other sanctions for offenses; state of health, illness, or disability of a person, or treatment or other comparable measures to which the person has been subjected; the sexual behavior of a person; and social services, economic support, social assistance, and related social welfare services received by a person);
(4) The obligation of the controller of the file to rectify erroneous data;
(5) Restrictions on delivery of personal data from a personal data file;
(6) Protection of a personal data file against unauthorized manipulation, use, erasure, and alteration, as well as against appropriation;
(7) Erasure of a personal data file which is no longer necessary;
(8) The right of inspection of personal credit and other data files by the person concerned; and
(9) The right of the person concerned to prohibit the use or delivery of data.

Clarification of the Scope of the Book

Some attention must be paid here to defining the scope of this book, because the problems created by the advent of the "information age" are too numerous to be covered by any one book.

The concept of "data" here is limited to "personal data". While the definition of personal data differs in detail from country to country, in general, it can be said to include any information relating to an identified or identifiable individual.

Furthermore, while the laws of some countries refer to data files which are not automated, in general, the laws described herein are concerned with automated data files and to automatic processing of personal data. In addition, while some laws refer only to such activity in the public sector, other laws cover the same activity in both the public and private sectors.

This book does not concern:

(1) The interception of communications over cordless or cellular telephones;
(2) Computer hacking;
(3) The monitoring of electronic mail (E-mail) of employees; or
(4) The electronic monitoring of workers themselves as they perform their jobs.

For information about the remedies to these and countless other problems born of the information age, the reader must turn to other sources.

Joy Fisher
Editor
Center for International Legal Studies
Salzburg, Austria

Notes

1. Quoted in Washburn, "Electronic Journalism, Computers and Privacy", Volume III, *Computer Law Journal*, p. 189.
2. *See* the introductory chapter, "The Council of Europe and the European Community."
3. *Id.*
4. It is interesting to note that, in Hong Kong, one of the major spurs toward adoption of a comprehensive data protection law is the concern that, without watertight legislation in place by 1997, when Hong Kong reverts to the People's Republic of China, there will be no safeguards against human rights abuses based on information derived from personal data by the future government.
5. Rothfeder, "Psst, Your Personal Details Are Getting Lots of Notice", *International Herald Tribune*, 14 April 1993, p. 9, column 7.
6. "Privacy Groups Fear Health-Care Data Bank", *International Herald Tribune*, 25 August 1993, p. 3, column 3.