Data Protection, Privacy and Freedom of Information

Dr. Prathiba Mahanamahewa

Mrs. G. I. Gamage

Introduction

- At the end of the twentieth century there can be very few people who remain unaware of the dramatic impact which increasing computerization has had on the storage, processing, retention and release of information and data.

- Computerization has revolutionized the handling and processing of information to such an extent that the data itself has now become a commodity which possesses commercial value and can be traded on the market in the same way as any other commodity.

•The value to businesses is also enhanced by the fact that data can be transferred around the globe with great ease.

•Personal data has been collected and held for a multitude of purpose throughout history with the consequent possibility of inappropriate or unauthorized use or disclosure.

•To quote Earl Ferrers, “(T)he collection of personal data is as old as society itself.

- It may not be the oldest profession but it is one of the oldest habits.

- A number of strands of concern emerge – the potential for abuse of organizational records, the incidental and often unwitting transfer of personal data.

- It is the issues raised by these factors which will form the subject matter of this chapter.

Data protection and privacy

- The discussion thus far has tacitly assumed that the reader is aware of what is meant by data protection and its relationship and interrelationship with the concept of privacy – a term even more elusive of definition.

- Since the first formulation of best practice at the beginning of the 1980s, many of the existing guidelines seem to either assume a connection or appear to use the terms interchangeable.

•Thus the Council of Europe Convention … whose declared object is to "strengthen data protection" then sets out in the article 1 that the purpose of the Convention is to "secure (the) right to privacy with regard to automatic processing of data".

•Such an apparently close relationship between data protection and privacy seems to have created a stumbling block in the legislative consciousness of the UK because of the lack of legal protection for privacy *per se* in this jurisdiction

- Although one of the antecedents of the data protection legislation in the UK , the Report of the Younger Committee on Privacy, conceded that increasing computerization could threaten privacy, the subsequent report of the Lindop Committee on Data Protection attempted to distinguish the two whilst at the same time agreeing that data protection could perhaps be equated with “information privacy”.

- Recent decision of the Data Protection Tribunal it was said that “(A)n underlying purpose of the data protection principles is to protect privacy with respect to the processing of personal data – a verbatim quote from article 1 of the Data Protection Directive.

- Further , both holders of the post of Data Protection Registrar to data have viewed their role as primarily one of the protecting individuals rights.

- In 1994, the first Data Protection Registrar, Eric Howe, said in his final report: "…data protection legislation is about the protection of individuals rather than the regulation of industry.

- It is civil rights legislation rather than technical business legislation, a declaration which might have seemed almost heretical in 1984.

- The matter might have been finally resolved with the implementation in the UK of the EC Directive on Data protection but, notwithstanding the tenor of article 1 of the data directive, the Data Protection Act 1998 never actually makes mention of the word “privacy” and it is clear from a number of debates in Parliament during the passage of the legislation that the connection between data protection and privacy is not accepted by all sides of the debates.

The impact of the Internet

- The original challenge of data protection law was to provide a suitable mechanism for dealing with the perceived threat to individual privacy of large centralized data banks and with abuse of information management made possible by techniques such as data matching.

- It has been suggested that “(T)he development of global information network has changed and intensified the character of the privacy protection problem”.

- The question which is inevitably being asked is whether the original formulation of data protection law is capable of controlling the amorphous decentralized activities which occur through the medium of the Internet and World Wide Web .

- In contrast to the situation for which data protection law was developed, this medium has no identifiable “data controller” in whom responsibility for safeguarding privacy can be invested.

•Of particular concern is the traceability of operations performed via on-line services together with a lack of general principles relating to the dissemination of information and protection of personal privacy.

•One central feature of the development of global networks such as the Internet is that a number of common features such as the ability to leave “navigation trails”, the existence of privileged websites, the use of “cookies” to capture and retain information about users and so on may effectively replicate other data matching processes.

•A further issue, as in many other branches of information technology law, is that of jurisdiction.

•Here the issue is one of correlation of personal data between organizations within the same jurisdiction, this may be dealt with appropriately by existing data protection legislation.

•The fact that data protection legislation usually contains provisions prohibiting trans-border data flow under certain conditions may also be useful in situation where the organizations are in different jurisdictions.

Factors influencing the regulation of data processing

- From the European or UK perspective, it is easy not to question the use of conventional legal devices to regulate this area.

- Legislation imposing sanctions backed up by action in courts and tribunals has, for a number of reasons, been the method chosen or imposed on these jurisdictions.

- Formidable problems of policy and implementation are presented by the attempt to regulate systems and practices that are technologically advanced, widely dispersed, rapidly changing and employed by powerful economic and government interests.

- Taking such factors into account, which regulatory strategy will be the most effective – the “top-down” approach of legislative intervention or the “bottom-up” approach of sectoral self-regulation? The use of such terminology implies conflicting philosophies, but it would , in fact, be misleading to imagine that these apparently opposing mechanisms are entirely mutually exclusive.

Younger principles

1. Information should be regarded as held for a specific purpose and should not be used without appropriate authorization for other purposes.

2. Access to information should be confined to those authorized to have it for the purpose for which it was supplied.

3. The amount of information collected and held should be the minimum necessary for achievement of a specified purpose.

4. In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.

5. There should be arrangements whereby the subject could be told about the information held concerning him.

6. The level of security to be achieved by a system should be specified in advance by the user and should include precautions against deliberate abuse or misuse of information.

7. A monitoring system should be provided to facilitate the detection of any violation of the security system

8. In the design of information systems, period should be specified beyond which the information should not be retained.

9. Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.

10. Care should be taken in coding value judgment.