Department of Geomatics
University of Cape Town
Private Bag
Rondebosch
7700

Privacy Protection in Geographic Information Systems:

Guidelines for the Protection of Privacy in GIS in South Africa

Submitted by: Renate Schreiber (SCHREN008)

Supervisor: Mr M. Barry

Terms of Reference:
This thesis is submitted in partial fulfilment of the requirements of the degree of Masters of Science (Appl.Sc.) in the Department of Geomatics at the University of Cape Town in September 1998. As part of the degree, this thesis is a half-dissertation in fulfilment of the requirements of course SUR525Z.

Declaration

I certify that this thesis is my own work and where appropriate I have acknowledged the work of others.

Signed by candidate

Signature Removed

Renate Schreiber
September 1998

Abstract

Personal privacy issues are relevant to the GIS community. The distribution and dissemination of personal data is greatly facilitated through GIS tools. The use of these tools has been expanded from traditionally geographical operations to applications in geodemographics, and it is particularly in geodemographics where the protection of privacy becomes an issue. This thesis examines existing privacy protection guidelines put forward by international commercial and governmental sectors; the current international position with regards to the protection of privacy is reviewed, and South African legislation pertaining to these issues is explored. On this basis, a set of privacy protection guidelines is developed which can assist GIS managers in South Africa in ensuring that data collection and management do not infringe on personal privacy.

Six sets of privacy protection guidelines were examined: the Organisation for Economic Co-operation and Development (OECD), the European Union, the Information Industry Association of the US, the Individual Reference Services Group of the US, the National Information Infrastructure of the US, and the Information Privacy Principles of Australia. It was found that the OECD guidelines of 1980 had generally been adopted as a privacy protection standard, and therefore guidelines developed after 1980 show guidelines similar to the OECD. The following five issues are all addressed to varying degrees in the reviewed guidelines and form a common base: data quality, purpose specification, security safeguards, openness, and individual participation.

The law of privacy in South Africa was explored by studying the case law pertaining to privacy. Three constitutional cases and 16 common law cases were reviewed with respect to the legal interpretation of the right to privacy. The legal influences extracted from the cases, firstly, were found to affect data

gathering methods and data use, and secondly, were found to clarify issues surrounding privacy expectations and the limitations of privacy. Firstly, regarding data gathering methods and data use, the law states that data gathering may not be secret, data subjects must be informed of the data gathering process, and data subjects must be in a position to give informed consent. Secondly, privacy expectations are based on confidential relationships, and the legitimate use of private data stemming from confidential relationships is limited. However, there are clear limitations of the right to privacy; the right of privacy can only be upheld when there were expectations of privacy, when there is no necessity of the privacy intrusion, when an individual can be identified by the published information, and when the data subject did not consent to the publication of the private facts.

Based on the reviewed guidelines, a reasonable set of objectives was proposed to facilitate the availability and implementation of the guidelines generated in this thesis. These include the regulating effect of guidelines on the use of information and the associated actions, the public availability of guidelines, and the compulsory compliance with the guidelines.

It was concluded that for the South African privacy protection context the OECD guidelines can provide a privacy protection framework for GIS managers in South Africa. The OECD guidelines contain the collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguard principle, openness principle, individual participation principle, and the accountability principle. Two further guidelines were proposed in this thesis: the education guideline, referring to the commitment to educating data subjects and data users about risks and implications of privacy infringements, and the guideline of minimisation of personal data collection and storage, referring to the potential prevention of privacy infringements by assessing the necessity of personal data collection and storage.

The effective implementation of the guidelines will depend on the methods used for enforcing adherence to the guidelines. Ideally, the formation of a

professional body for GIS in South Africa will facilitate the implementation of privacy protection guidelines through the generation of professional information policies.

Contents

Acknowledgements

I wish to thank the following people for their contributions and support which made the completion of this thesis possible:

Mike Barry for his supervision

Bill Cargill for making it possible for me to 'work and study'

Adrian Charles for his patience

Antoinette Cloete for her availability

Jeremy Nel for his proof-reading

Birgit Schreiber for her critical thoughts

Note on Referencing Used in this Work

The references in this thesis include references from books and journals, from the Internet, and from legal cases. The three different referencing conventions used are outlined below:

1. Books and Journals:

   The Harvard Referencing method is used for books and journals both throughout the text and in the bibliography.

2. Internet Sources:

   The bibliography contains a separate section on Internet Sources used in this thesis. The alphabetical list is based on publisher and numbers the web sites with a 'Ref' Number. Throughout the text, the referencing contains the name of the Publisher of the Web site, Year of Website, and the 'Ref' number.

3. Case referencing:

   The thesis contains a Table of Cases which lists the complete details of the case, including the year and court. Throughout the text, only the names and the year is quoted. For verbatim quotes, the paragraph number in the law report is referenced in square brackets [].

Glossary of Terms

Boni Mores:
An opinion which reflects society's prevailing ideas and norms of what is regarded reasonable and proper.

Data Controller:
"A party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf", where 'domestic law' refers to the law of the OECD member states (Part 1.1.(a), OECD, 1980 Ref 22).

Data Protection:
The term 'data protection' is more prevalent in continental Europe, and refers to what in English speaking countries is termed 'privacy protection' (OECD, 1980 Ref 22). In this document the two terms are used interchangeably.

Delict:
A delict is defined as "the act of a person which in a wrongful and culpable way causes harm to another" (Neethling *et al*, 1994).

Injuria:
The wrongful and intentional infringement of an interest of personality.

Legal right::
A legal right is "an interest conferred by and protected by the law, entitling one person to claim that another person or persons either give him some thing or do an act for him or refrain from doing an act" (Barry, 1998).

Non-public Record:
This refers to information about an individual that is not available to the general public and is of a private nature, such as health records.

Personal Data:
This refers to any information relating to an identified or identifiable individual (data subject) (Part 1.1.(b) OECD, 1980 Ref 22). The Australian Privacy Act defines 'personal information' to mean "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" (Commonwealth of Australia, 1996, Ref 2).

Public Information / Public Record:
This refers to information about an individual open for inspection by the general public, or from data sources available to the general public, such as telephone directories, real estate records, court records, etc. (Federal Trade Commission, 1997, Ref 11).

Real Right:
See Legal Right

Tort:
see Delict

Chapter 1

1.1 Introduction

Personal privacy issues are relevant to the GIS community. The power of GIS allows the distribution and dissemination of information to an extent like never before. Information is not only distributed at a rapid rate, but also generated in ways which previously were not economically viable. The use of GIS tools has been stretched from their traditional use in geographical operations to the application of GIS in geodemographics. It is particularly in the field of geodemographics where the protection of privacy has become an issue, as there is evidence that individuals feel concerned and even threatened about to their personal privacy.[1]

The rate of improvement of computer power has now caused a dependence on systems and a vulnerability to electronic errors due to advances in data storage, advances in data mining techniques, and advances in telecommunication infrastructures. These forces are largely controlled by the professional or business class. They also enable potentially uncontrolled invasions of privacy and the potential propagation of errors in personal data through automated processing (see for instance Electronic Frontier Foundation, 1997, Ref 4).

Information has become a "potential source of wealth rather than simply a cost of doing business" (MacLean, 1984, cited in Anderson & McLaughlin, 1993). Geographical information can aid in the physical location of data or individuals, and the perceived threat of a privacy invasion may be heightened by attaching co-ordinates to facts and records. The combination of previously separate types of data - spatial and attribute - also feed this perceived

[1] For instance, the selected results of the 1992 Ekos survey "Privacy Revealed - the Canadian Privacy Survey" were quoted in Industry Canada (http://info.ic.gc.ca/info-highway/ih.html). The survey "... showed that while 52 percent of Canadians are extremely concerned about privacy, 92 percent expressed at least moderate concern. Moreover, 83 percent strongly believe that they should be asked for their permission before an organisation can pass on information about them to another organisation, and 71 percent totally agree that privacy rules should apply to both government and business."

threat. While access to data can contribute to an efficient government, it can mean a threat to the individual's privacy, which is why a balance between the two must be reached.

Land information in particular must receive special attention in this issue surrounding privacy. It is noted that until recently it has not been included in the list of 'privacy-threatening information'. This might be due to the focus on the *land* component in the information, where personal information seems secondary and mostly administrative. It might also be because most land information is stored in public databases and is therefore considered public information (Anderson & McLaughlin, 1993).

Neethling *et al* (1996) reports on factors such as the sociological revolution which caused the development of a complex urban society, the technological / industrial revolution fostering expansions in the mass media, and ideological developments promoting the awareness of privacy in society. Such developments have led to privacy being recognised as a fundamental human right.

There exists a danger of overplaying the protection of privacy. Protecting the individual's privacy entails the protection of the individual's sense of solitude, autonomy, anonymity and individuality (Alpert, 1995). However, this does not mean that the release of any personal information constitutes an invasion of privacy. "The protection of personal data is not the issue; rather it is the protection of privacy" (Anderson & McLaughlin, 1993:124). While the individual's concerns regarding the protection of privacy need to be heeded, there are other interested parties who can benefit from data contained for instance in government data banks, such as social scientists and other research users (Flaherty, 1979). Once again, the balance is important.

The type of practices that threaten the privacy of individuals are wide ranging in nature, and include the methods of data collection (such as the commercial availability of 1m resolution satellite images), record matching (such as the information held by the banking or insurance sector which can be address matched), the unintended use of personal data, unlawful storage of data, and the storage of inaccurate data. These are only a few factors contributing to

the complex issues surrounding privacy protection and privacy concern by individuals, and intensify the need for a solution.[2]

1.2 The research questions

A review of the South African legislation reveals that there is no explicit law regulating the protection of privacy with regards to information systems and computerised record-matching. There is a lack of enforceable guidelines preventing the infringement of privacy. The aim of this study is to generate guidelines and raise awareness within the GIS community regarding the protection of privacy.

Two questions are addressed in this study:

1. What guidelines can be developed to assist the GIS Manager to ensure data collection and management does not infringe on personal privacy?

This question relates to the moral and ethical aspect of privacy protection, and how this aspect is addressed in the general body of privacy protection guidelines.

2. What guidelines can be developed to ensure projects are implemented within the confines of the law of privacy?

This question relates to the issues surrounding privacy protection within the law. In order to appreciate the issues, the legislation of various countries is discussed. Of necessity, the South African law of privacy plays a particular role in developing local guidelines.

[2] A recent opinion poll, reported by Laudon & Laudon, completed in the United States had 76 % of the population feel they have lost all control over personal information and 67% believe in the need to restrict computer power to protect privacy in the future (Laudon & Laudon, 1996).

1.3 Structure of thesis

In attempting to answer the research questions the following method is adopted: to develop a literature background to the issues surrounding privacy protection guidelines, to establish what privacy protection guidelines exist, to find out about international and South African legislation surrounding privacy issues, and finally to develop a set of privacy protection guidelines which are suitable for the South African GIS context.

The thesis has the following structure:

1. Chapter 1 outlines the research questions, states the assumptions, limitations and biases of the thesis, and describes the value of this study.
2. Chapter 2 contains a literature review and a definition of terms; the literature review discusses previous work done on the issues surrounding privacy protection guidelines.
3. Chapter 3 outlines the research methods.
4. Chapter 4 contains the research data of the thesis. Section 4.2 discusses existing privacy protection guidelines published by various bodies of authority, section 4.3 considers the law of privacy as protected in international legislation, section 4.4 examines the South African law of privacy, and section 4.5 explores South African case law relating to privacy and analogous situations.
5. Chapter 5 analyses the legal influences on privacy protection guidelines as imposed by the South African law of privacy, and the effect of legislation on the way data can and cannot be used. Objectives of privacy protection guidelines are formulated. A set of privacy protection guidelines for GIS in South Africa is developed.
6. Chapter 6 discusses the conclusions drawn in the study and states recommendations.

1.4 Assumptions and limitations

At present, there is no official professional association for GIS, which makes the process of enforcing guidelines difficult if not impossible. Guidelines will only be effective if infringements are followed by punitive action, or if infringements cause the revoking of membership from a professional association. This would only be effective if the association was providing substantial benefits to its members.

The guidelines are not intended to protect medical records. It is assumed that the medical sector has more specific requirements for the protection of personal data, which are not intended to be covered by the guidelines suggested in this thesis. These guidelines are intended to apply to personal records, such as personal data used in the marketplace, banking records, financial records, credit information, identity numbers, personal property, telephone records, lifestyle information, etc.

The countries for the literature research were chosen on the basis of being advanced Western democracies with experiences most likely to be relevant to the South African situation. This is not to say that there are no other countries with privacy legislation that South Africa could benefit from. The representative sample was chosen by the author to obtain as broad a view as possible.

This study focuses on existing legislation and guidelines, and does not attempt an in-depth examination of the ethical issues surrounding privacy protection.

The guidelines developed in this thesis have not been tested in the field with regard to their applicability and the practicality of their implementation. This is due to time limitations and the fact that it is beyond the scope of this half-thesis. The applicability and practicality could be tested by means of discussions and interviews, and by 'work-shopping' the guidelines with professionals in the field. It must be remembered that the effectiveness of

guidelines is dependent on their implementation in a way which enables compliance and enforcement.

1.5 Research Bias

This research findings are biased by the author's personal, subjective analysis. Furthermore, throughout the research it became apparent that the privacy protection guidelines developed after 1980 are based substantially on the privacy protection guidelines put forward by the Organisation for Economic Co-operation and Development. This single root to guideline development is regarded a bias in the guidelines researched in this thesis.

1.6 Value of this research

This study will draw attention to the problems surrounding existing South African legislation regarding the protection of privacy. It is intended to serve as a reference document guiding the implementation process involving GIS projects, assisting in avoiding unlawful methods of data acquisition and data dissemination which may attract litigation.

Chapter 2: Definition of Terms and Review of Previous Work

2.1 Introduction

This chapter contains a definition of terms and states operational definitions for the concepts of privacy and personal data. The development process of privacy protection guidelines is illustrated. Furthermore, this chapter reviews previous work done on the issues surrounding privacy protection guidelines and shows how other researchers have approached the issue. The OECD guidelines are briefly reviewed, as they form the basis for the developments in privacy protection guidelines since 1980. The issues surrounding the development of privacy guidelines as approached by a number of other researchers are outlined. The influence of self-regulation as an alternative to legislation in privacy protection is discussed.

2.2 Definition of Terms

2.2.1 Privacy

From a sociological or psychological perspective 'private' can be defined as the "elective control of access to the self or one's group" (Altman,1975, cited in Fisher, Bell & Baum, 1984:276). In today's information age, there seems to be a need to extend this definition to include aspects of personal data, so that privacy refers to the "ability to withdraw ourselves from other people" and the "ability to control information about ourselves" (Fisher *et al*, 1984:276).

Neethling *et al* (1996) defines privacy as "an individual condition of life as characterised by exclusion from publicity. This condition includes all those personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy" (*ibid.*:36).

Westin (1967) provides the following definition of privacy: Privacy is "the claim of individuals, groups, or institutions to determine for themselves when,

how, and to what extent information about them is communicated to others." (cited in Wacks, 1993:84).

The above definitions suggest that the most crucial components of privacy are the individual's ability to decide when to be left alone and to be free from intrusions, and the ability to exercise control over one's personal information. The operational definition of privacy adopted for the purpose of this study is Westin's definition.

2.2.2 Personal Data

The definition of 'personal data' or 'personal information' is more complex than it may seem at first glance. It can be defined as "any information which relates to any data subject who is, or can be identified – including the information whereby he can be identified" (Younger Commission, UK, cited in Wacks, 1980:125). However, Wacks (1980) proceeds to point out the dilemma which arises from such a broad definition – it includes virtually any data about an individual – and criticises this approach to privacy protection, where "by conceiving 'personal' to mean not 'private' but 'of the person', the subject is even further muddled" (*ibid.*:125).

Wacks (1980) thus defines personal information as "those facts, communications or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or confidential and therefore to want to withhold or at least to restrict their circulation" (*ibid.*:22). This definition can offer more effective protection against the misuse of personal data, which can then in effect offer protection of an individual's privacy.

The German *Bundesdatenschutzgesetz* (Federal Data Protection Law) defines personal data as referring to "details on the personal or material circumstances of an identified or identifiable physical person" (BDSG, 1977, § 2 (1)), drawing specific attention to the ability to *identify* a person, making the definition more all-encompassing.

For the purpose of this thesis the terms 'personal data', 'personal record' and 'personal information' are used interchangeably. They refer to data relating to an individual which has an expectation of privacy attached, and which an individual can reasonably expect to have a right of control over.

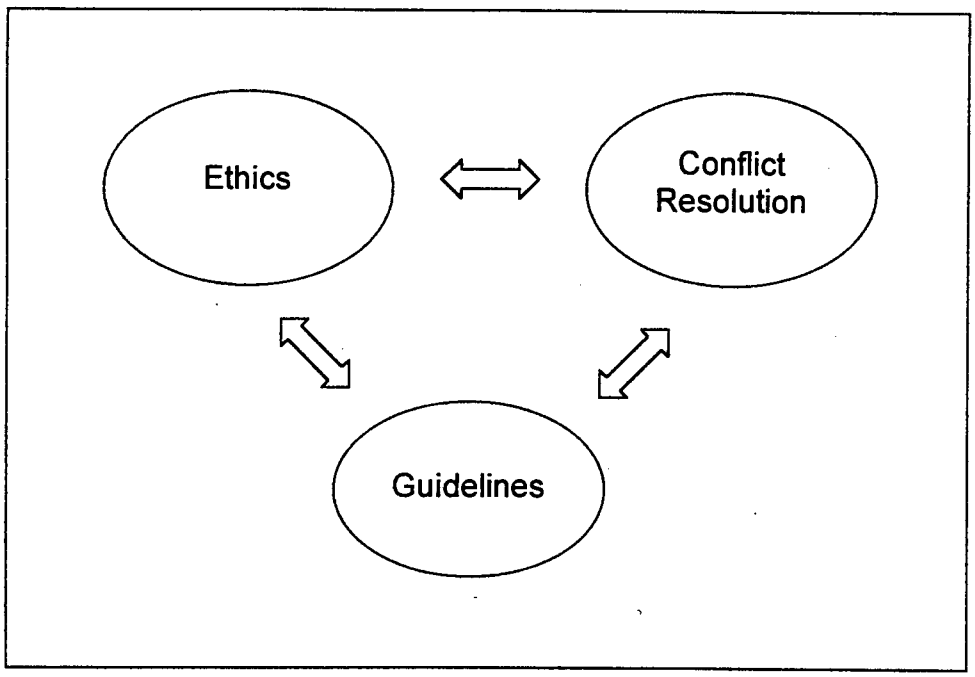
2.3 Privacy Protection Issues

2.3.1 Ethics in Information Systems

Ethical, social and political values are affected by the developments taking place in the field of information systems, privacy being one of these issues. Similar to legal issues, the rate of development for ethics and morals is slower than the rate of development in new technology; even some 20 years ago some critics contended that technological advances have surpassed social control (Flaherty, 1979). No guidelines had been established to protect individuals against harmful effects of the technological developments.

Ethics form part of the development process of privacy protection guidelines, illustrated in Figure 2.1. Ethics reflect society's customs and norms, and influence perceptions of what is regarded personal information. Guidelines emanate from ethics and should contain a set of factors guiding the implementation of ethical practice. Conflict resolution involves law cases and arbitration, and reflects the ethical standards of the law. The non-static nature of ethics causes a continual interaction between the ethics, guidelines and conflict resolution. The nature of guidelines should therefore be operational, and can be expected to change to mirror the ethical standards that apply at a particular time (Barry, 1998).

Figure 2.1 Cyclical Process of Privacy Guidelines Development



In this thesis the focus lies on the generation of guidelines as affected by conflict resolution, i.e. law cases and arbitration. In the literature review, the ethical and moral aspects of privacy protection are also addressed.

Based on the literature surrounding ethical, social and political issues in information systems, Laudon & Laudon (1996) isolate the following five 'moral dimensions' which relate to the moral concerns in the information industry:

- the issue of information rights and obligations (protection and obligations)
- the issue of property rights (intellectual)
- the issue of accountability and control (who is responsible / liable)
- the issue of system quality (security)
- the issue of quality of life (what values/practises are protected in new information technology)

Specific ethical questions surrounding the issue of privacy include the extent to which an invasion of privacy is justified, what kind of collection methods are

appropriate, and the amount of information given to data subjects about the use of their personal data. Social privacy concerns relate more to aspects of personal territory and the levels of expectation of privacy. Since these issues are often not addressed by legislation, guidelines of codes of conduct can assist in data collection and management (Laudon & Laudon, 1996).

2.3.2 Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD) consists of 24 leading industrialised nations of the world. In 1980 a set of privacy guidelines was adopted, a summary of which follows below. The body of literature researched contains substantial references to the OECD guidelines[3] , and they seem to have formed the basis of most sets of guidelines developed after 1980 (Onsrud *et al*, 1994). Thus, it seems sensible here to provide the reader with a summary of the core principles:

1. *Collection Limitation Principle*: There should be limits on the collection of information. Collection should be lawful, fair and with the knowledge and consent of the individual.
2. *Data Quality Principle*: Data should be relevant, accurate, complete and up-to-date.
3. *Purpose Specification Principle*: The purpose for collection should be stated upon collection; the use of the data should be limited to this purpose.
4. *Use Limitation Principle*: There should be no secondary uses of personal data without the consent of the subject, or without authorisation by the law.
5. *Security Safeguards Principle*: The data should be protected by the collector.
6. *Openness Principle*: A general policy of openness should be adopted regarding development, practises and policies.

[3] See Appendix 1 for a copy of the OECD guidelines, and Section 4.1.1 for a discussion.

7. *Individual Participation Principle*: Data subjects should be entitled to inspect and correct data and determine the data file existence.
8. *Accountability Principle*: Data controllers should be held accountable for complying with these guidelines.

These guidelines are not enforced by the law. They are aimed at increasing the awareness and improving the practises related to information systems.

2.3.3 Development of Privacy Protection Policies

Based on the OECD guidelines, Anderson & McLaughlin (1993) developed a list of factors which should be addressed when developing a set of guidelines for the protection of privacy, irrespective of the legal situation impacting on privacy protection:

- Are the socio-political objectives met by the information regulation?
- How does the regulation fit into the social and traditional patterns of a jurisdiction?
- How will advances in information technology affect regulation?
- Are they media independent to accommodate advances in technology?
- Are they applicable to all sectors of society?
- Are privacy and access considered coincidentally?

Anderson & McLaughlin (1993) proceeds to list the components which should in all cases be present in policies relating to the protection of privacy. What follows is a selection of these components:

- Commitment to information access: including a statement of priority placed on providing access to information products and services
- Access mechanisms: description of media independent access control categories, specification of technical standards
- Equity: provision of equitable access to information

- Privacy: statements and declarations relating to the importance of the value of privacy, the balance of quality of access and privacy, the controls established to protect privacy
- Security: statement of appropriate security provisions, highlighting the security responsibilities of both the data custodians and information users[4]
- Information ownership: statement of the rights and responsibilities that come with information, redistribution of information to third parties
- Pricing: specification of tangible and intangible costs and benefits in the provision of information
- Role of the public and private sectors: recognition that roles of involved sectors may change over time
- Liability: custodial responsibilities, obligations of parties involved, and the limit of liabilities.[5]

2.3.4 Self-regulation

The commercial sector is generally encouraged to show self regulation in their activities (Flaherty, 1994; Alpert & Haynes, 1994; Raab, 1994). Flaherty (1994) in particular sees the encouragement of self-regulation as an alternative way of bypassing the problem of legislation; in many countries legislation has not managed to keep up with the rapid advances of technology, and therefore encouraging the commercial sector to achieve effective self-regulation may be a faster solution to the problem. Raab (1994) questions the effectiveness of self regulation without empirical demonstration. An example of self-regulation is to be found the banking industry in the United States, which has chosen *not* to utilise data generated from Automatic Teller Machines for marketing purposes. This is not a restriction imposed by the law, rather, the importance of assuring the customer of the integrity of the ATM system has led to banks adopting this policy as a protection of the privacy of their customers (Alpert & Haynes, 1994).

[4] It must be noted here that security of information systems is in itself a complex and debatable issue, the discussion of which is not included in this thesis.

Lopez & Onsrud (1994) facilitate the encouragement of self-regulation by actually supplying a number of steps which can be followed by GIS administrators and designers to ensure fair information practises. These steps include the establishment of privacy protection policies and the clear definition of sensitive data, much like most other privacy protection guidelines. The fact that they stress the importance of privacy to staff and the involvement of public participation indicate a new approach in the scope of privacy protection guidelines. The relevance to privacy protection guidelines here is that steps such as these which facilitate self-regulation can complement the effect of privacy protection guidelines.

2.3.5 Other Factors

G.T. Marx (1994), a social scientist, compiled a list of sixteen privacy protection principles, most of which coincide with guidelines such as the OECD. Unique to his list is the principle of 'human review of machine decisions'. This highlights the fact that with the databases we are dealing with, computers cannot make decisions on privacy issues - it is the user who must keep the principles in mind.

Epstein (1991) makes an interesting distinction regarding the values governing the system of information access and flow:

- Public values: the desire by citizens to know how the government is operating and what it is up to. This is as a result of a fear of totalitarianism where the government's control over citizens might be encouraged through confidential information systems.
- Private values: the concern of citizens about the revealing of private information.
- Commercial values: Site-specific and comprehensive data is specifically pointed out as commercially interesting data. Data is treated like other commodities.

[5] Liability is a complex topic of legal debate, and its discussion is not included in this thesis.

The relevance to privacy protection here is how these three values can be integrated into privacy protection guidelines. Privacy is affected by the ways in which these values are upheld, as under certain conditions private values can become a casualty of the pursuit of public values. Commercial values can cause privacy infringements when the economic interest in data overrides private values.

2.4 Summary

This chapter provides operational definitions for privacy and personal data. Existing research surrounding issues of privacy protection is reviewed. The development process of privacy protection guidelines is discussed. This chapter provides a background to the development of privacy protection guidelines, and illuminates alternative approaches to the issues at hand. As an alternative to privacy protection guidelines, Anderson (1992) for instance compiled a list of factors to be addressed when developing guidelines. Anderson (*ibid.*) also lists some components crucial to an information privacy policy. Self-regulation with its benefits and problems is also reviewed as an alternative approach to structured privacy protection guidelines. The potentially conflicting values governing the system of information access and flow are discussed, illustrating the significance of balancing this system in order to prevent privacy infringements.

Chapter 3: Research Methods

The framework of data collection and analysis adopted for this study is a desktop study and analysis. Figure 3.1 depicts the process leading to the development and evaluation of a set of guidelines derived from the literature.

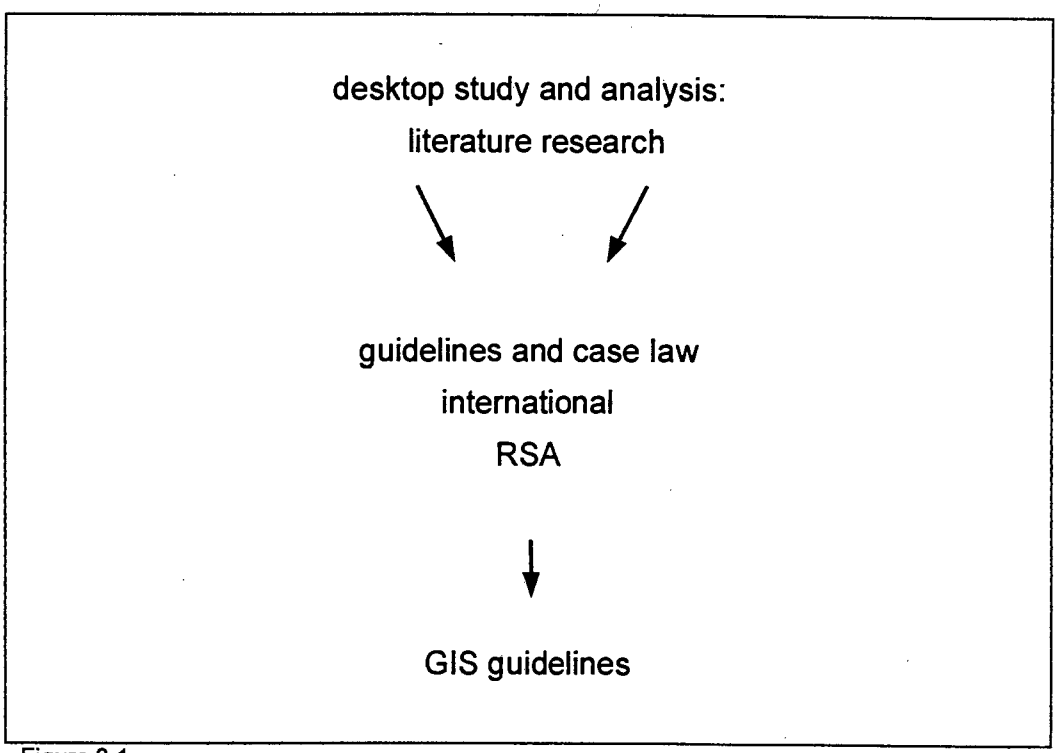


Figure 3.1

The initial stage consisted of data collection through in-depth literature research. Existing privacy protection guidelines were examined. Focus was placed on selected European countries and organisations, the USA, Canada, and Australia on the basis of their approach to privacy protection.

The second stage of data collection entailed South African case law research. Case law pertaining to privacy was reviewed and judgements investigated. The aim was to study how privacy is protected in South Africa under existing legislation, and how this legal protection influences the way in which data can be used in South Africa so as not to infringe on personal privacy.

Based on international experience and on the South African legal position with respect to privacy, a set of guidelines was constructed. The guidelines were envisaged to be applicable for GIS managers for guiding the GIS implementation and data collection process.

Limitations and biases of this study are described in section 1.4 and 1.5 respectively.

The study was intended to follow an interpretative approach, with the aim of solving as well as constructing research questions.

Chapter 4

4.1 Introduction

This chapter contains the research data of the thesis. Firstly, six existing privacy protection guidelines as published by various bodies of authority are discussed. This includes the OECD, the European Union, the Information Industry Association of the US, the Individual Reference Services Group of the US, the National Information Infrastructure of the US, and the Australian Information Privacy Principles. Secondly, the law of privacy as protected in international legislation is considered, in order to provide a background to the discussion on the South African law of privacy, which is discussed in the following section. Finally, South African case law relating to privacy is explored in order to generate an understanding of how privacy is protected in South Africa under existing legislation. The influence of South African case law on data collection and use will then be analysed in Chapter 5.

4.2 Existing guidelines

4.2.1 Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD) has developed privacy protection guidelines to protect individuals against violations of their fundamental human right to privacy and individual liberty. The focus is twofold:

1. to protect the individual against actions such as the unlawful storage of personal data, storage of inaccurate data, abuse or unauthorised disclosure of personal data
2. To facilitate transborder flow of data; discrepancy in privacy laws presents a threat to the transborder flow of data

The member states are encouraged to harmonise legislation to ensure that domestic legislation does not interfere with the social and economic benefits of the transborder flow of data. The OECD does not have the legislative

power to influence exactly how their member states comply with the guidelines and is potentially faced with the disproportionate application in different countries (OECD, 1980, Ref 22).

The development of the OECD guidelines was prompted by the need for the harmonisation of national legislation which, in the 1970s, concentrated strongly on protection of privacy. The guidelines, issued in 1980, offer a minimum standard of privacy protection and member states are encouraged to use self-regulation and to provide adequate sanctions and remedies in cases of transgression. The guidelines should not be applied in a mechanistic, 'hard-and-fast' way, but rather to each situation in a suitable way, respecting the varying degrees of sensitivity of data. The OECD stresses the need for international consensus on the fundamental principles of privacy protection in order to reap the benefits of today's global technological advances without presenting a threat to basic human rights (OECD, 1980, Ref 22).

The following principles form part of the OECD guidelines[6]: (OECD, 1980, Ref 22)

1. Collection Limitation Principle

   Collection of personal data should be limited and should follow lawful and fair practices, and with the knowledge or consent of the data subject.

2. Data Quality Principle

   Personal data should be relevant to the intended purpose, and it must be accurate, complete and kept up to date.

3. Purpose Specification Principle

   The purpose for data collection should be specified at time of collection. The use of the data must be limited to this purpose or

[6] See Appendix 1 for a copy of the complete document released by the OECD.

to related purposes, where related purposes must be compatible and specified on each occasion of change of purpose.

4. Use Limitation Principle

Use of data should be limited to the use for the specified purpose. It may only be used for another purpose if the data subject agrees to alternative use, and if the law allows it.

5. Security Safeguard Principle

Personal data should be safeguarded against risks such as loss, unauthorised access, destruction, use, modification or disclosure.

6. Openness Principle

There should be a general principle of openness regarding the developments, practices and policies with respect to personal data. Information regarding the existence, nature and purpose of personal data must be accessible, as well as information regarding the identity and residence of the data controller.

7. Individual Participation Principle

Individuals should have the right to establish the existence of data relating to them, have this data communicated to them in a reasonable format, within a reasonable time frame and for a reasonable charge. Should this right be refused, the individual should be entitled to challenge this refusal, to challenge the data, and if the challenge is successful, to have the data removed or rectified as requested.

8. Accountability Principle

> The data controller should be accountable for conforming to the guidelines which give effect to the principles stated above.

The Collection Limitation principle can be difficult to apply in the sense that consent of the subject cannot always be obtained (OECD, 1980, Ref 22). While it prohibits data collection such as the concealed use of tape recorders, there are certain methods such as routine updating of address lists which might not require the actual consent of the individual. At all times, it refers at least to the individual's knowledge that a particular record is kept.

The Individual Participation principle is regarded as the most important safeguard against infringements (OECD, 1980, Ref 22). The right of access to records by an individual should be easy to execute and not be hindered by impracticalities on the side of the data controller. This highlights the prominent difference between the OECD guidelines and the Information Industry Association's approach (see section 4.2.3), where the latter maintains that such individual verification requests are not practical to entertain.

The Accountability principle is intended to avoid data controllers shedding their responsibility regarding privacy protection based on the fact that they are working on behalf of another party. Every data controller is therefore bound to specific data practises, and this is extended to the party the data controller is representing. This means that in cases of transgressions, both the data controller and for instance the service bureau they are working for can be held responsible for the transgression.

In a recent workshop entitled "Privacy Protection in a Global Networked Society" held by the OECD, the Internet received special attention.[7] (OECD,

[7] It should be noted here that the World Wide Web consortium has shown concern with respect to privacy on the Internet. A special project called the P3P has the following focus: "The Platform for Privacy Preferences Project (P3P) will result in the specification and demonstration of an interoperable way of expressing privacy practices and preferences by Web sites and users respectively. Sites' practices that fall within the range of a user's preference will be accessed "seamlessly", otherwise users will be notified of a site's practices and have the opportunity to agree to those terms or other terms and continue browsing if they wish" (W3C, 1997, Ref 28). The reader is referred to the Electronic Frontier Foundation, 1997 Ref 4, for the latest version of the Electronic Frontier Foundation Policy on Public Interest Principles for Online Filtration, Ratings and Labelling Systems which relates to the work done by P3P.

1998, Ref 23) It is stated that in order to uphold privacy protection on the Internet and the World Wide Web, and at the same time ensuring the benefits of free flow of information, the following aspects need to be balanced:

- education and transparency
- flexible and effective instruments
- potential benefits of technology
- enforceability and redress

This illustrates the OECD's commitment to keeping up with the demands placed on privacy protection by technological advances.

4.2.2 European Union

There is a movement towards harmonising the national laws relating to privacy and the distribution of information (Lopez & Onsrud, 1995). Difficulties have been experienced due to national and cultural differences in the definition of privacy. The European Union is aiming at consistency with regards to the law of privacy in its member states to facilitate data transfer.[8]

The European Union adopted a Directive (directive 95/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (European Union, 1995, Ref 8). The Council encourages closer relations between the member states, both economically and socially, and thus recognises the need to offer some form of regulation with regard to the processing and transmission of personal data amongst the member states and to non-member states. The Directive provides protection principles which apply to personal data, either processed automatically or

[8] The EU has issued the deadline of 25th October 1998 for EU states to implement policies protecting citizens from "computer-age invasions of privacy" (Independent Newspapers, 1998, Ref 14). The directive, known as European Data Protection Directive, enables citizens to decide about the existence and use of their personal information. This is envisaged to have a major impact on international information trade relations as it prevents organisations from transferring personal data to third organisations who do not show adequate levels of protection, and highlights the need for a global solution to data privacy.

stored in a filing system allowing easy access, excluding personal data processed by a natural person for purely personal or household activities.

The following is an extract from the Directive, focussing on issues regarded as more relevant to the generation of guidelines[9]:

Article 6 stipulates the following principles for *data quality*:

1. Processing must be fair and lawful.
2. Purposes for collection must be explicit and legitimate, and further processing must fall within the bounds of these purposes.
3. Personal data must be adequate, relevant and not excessive in relation to the stated purposes.
4. Personal data must be accurate and kept up to date. Inaccurate or incomplete data must be erased or rectified.
5. Personal data leading to the identification of data subjects must be kept for no longer than is necessary for the stated purposes. Specific safeguards are required for data used for historical, statistical or scientific use.
6. It is the data controller's responsibility to ensure that points 1. to 5. are complied with.

Article 7 stipulates the following principles relating to the conditions under which data processing is legitimate:

1. The data subject has given his consent unambiguously.
2. It is required for compliance with a legal obligation.
3. It is necessary in order to protect the vital interests of the data subject.

[9] See Appendix 2 for the complete document as released by the Council of the European Union.

4. It is necessary for the performance of a task carried out in public interest, if such interests are not outweighed by the interests or fundamental rights and freedoms of the data subject.

Article 8 stipulates the following special *categories of data processing*:

1. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, concerning health or sex life, may not be processed.
2. Paragraph 1 does not apply where the data subject has given their explicit consent.
3. Paragraph 1 does not apply where processing is necessary in the field of employment law (provided adequate safeguards are given by the national law).
4. Paragraph 1 does not apply where processing is necessary to protect the vital interests of the data subject and the data subject is physically or legally incapable of giving their consent.
5. Paragraph 1 does not apply where processing is carried out by a non-profit organisation with appropriate guarantees and in the course of its legitimate function of political, philosophical, religious or trade-union nature.
6. Paragraph 1 does not apply where the personal data are manifestly made public by the data subject, or is necessary for the establishment, exercise or defence of legal claims.
7. Paragraph 1 does not apply where processing is required for the purpose of preventative medicine and related purposes, where the processing is supervised by a health professional.

Article 9 states the following with regard to *freedom of expression*:

The processing of personal data solely for the purpose of journalistic, artistic or literary expression could only be permitted in a situation where the author's/artist's freedom of expression would be deemed to have outweighed the right to privacy.

Article 10 states that the following must be revealed to the data subject when personal data is collected *directly* from the data subject:

1. The identity of the data controller must be revealed.
2. The intended purposes of the data processing must be revealed.
3. The recipients (or categories of recipients) of the personal data must be revealed.
4. It must be stated whether the data subject's responses are obligatory or voluntary, and any consequences of failure to respond must be explained.
5. The existence of both the right of access to and the right to correct data must be made known.
6. The above information must be supplied when necessary to guarantee fair processing.

Article 11 states the following must be revealed when personal data is *not* obtained from the data subject:

1. The data controller must, at the time of recording or at disclosing the data to a third party, undertake to inform the data subject of the identity of the data controller, purposes for processing, categories of data concerned, recipients or categories of recipients, the existence of the right of access and the right to correct potential errors.
2. Paragraph 1 does not apply where the data is used for statistical purposes, historical or scientific research purposes, or if the provision of the information requires a disproportionate effort.

Article 12 states the following with regard to the *right of access to data*:

1. The data subject has a right to be informed of whether data relating to them is processed, or at least the purpose of processing, the categories of data concerned, and who the recipients will be.
2. The information shall be communicated in an acceptable form.
3. The method and/or logic of processing shall be disclosed in cases of automatic processing.

4. The data subject has a right to demand the rectification or erasure of incomplete or inaccurate data. Recipients of the data shall be informed of such rectification/erasure, unless disproportionate effort is required to do so.

Article 13 provides for various exemptions in areas such as national security, criminal investigations, and budgetary and taxation matters.

Article 14 states the following with regard to the *right to object*:

1. The data subject has the right to object to the processing of their personal data in cases where the data controller expects the data to be used for direct marketing.
2. The data subject has the right to object to the disclosure to third parties where the data will be used for direct marketing purposes.
3. The data subject has the right not to be subject to a decision which can significantly affect him, for instance creditworthiness, conduct, etc., where such decisions are solely based on automatic processing.

As with the OECD guidelines, the European Union's Directive provides for control over the transfer of personal data to non-member states (Article 25). This encourages non-member states to set up a privacy protection framework to maintain data flow with EU member states (Federal Trade Commission, 1996, Ref 10).

The format in which the EU Directive deals with the use of personal data is much more detailed than for instance the OECD guidelines. It addresses special occurrences of data use and data dissemination individually, while the OECD issues a clear set of guidelines which is qualified in an associated recommendation. The application of the EU Directive within the GIS community would prove to be far more complex and potentially less successful than the implementation of a clear set of guidelines. It is argued that the complexity of guidelines affects the way in which they can be included

in the procedures of data collection and management, and in analysis of this, the format of the OECD is preferred.

4.2.3 Information Industry Association (US)

The Information Industry Association (IIA) represents hundreds of companies involved in marketing 'information-rich products', such as publishers, telecommunicators, and credit bureaux. The association put forward Fair Information Practices Guidelines together with a Privacy Policy Statement and Fair Information Practices Checklist.[10] While the Fair Information Practices Guidelines coincide to some extent with those put forward by the OECD, the stance taken towards the guidelines is different. In response to the Federal Trade Commission's study on databases and Consumer Privacy in December 1997, the IIA has outlined some of its' attitudes towards privacy protection guidelines (Federal Trade Commission, 1998, Ref 13). [11]

It is the IIA's opinion that the free flow of information must be supported and restrictions should only be targeted at cases of proven consumer harm. The IIA argues that authorities such as the Federal Trade Commission are too concerned with consumer privacy *concerns*, rather than with *harm*. According to the IIA, there is great discrepancy in public opinion regarding privacy concerns. For instance, there is the concern about public access to Social Security Numbers, yet these numbers are readily supplied by individuals in the US in arbitrary cases such as cashing a cheque. Another example quoted is one where consumers regard the 'spamming' of e-mail addresses as a privacy intrusion, yet regard it as harmful to be excluded from certain offers by e-mail. The IIA feels that this discrepancy in consumer attitudes makes the

---

[10] See Appendix 3 for the complete Fair Information Practices Guidelines as released by the Information Industry Association.

[11] The Federal Trade Commission (FTC) is regarded as the most 'privacy active' agency in the United States (National Information Infrastructure Task Force, 1997, Ref 21) and has served as a significant source of information for this thesis. "The mission of the FTC is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and increasing consumer choice by promoting vigorous competition. The Commission undertakes this mission by enforcing the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce" (Federal Trade Commission, 1998, Ref 13). Rather than discussing the FTC's approach to privacy protection here, the reader is referred to the FTC homepage Ref 9 for a comprehensive report.

attempt of protecting against consumer privacy concerns very frustrating, and such attempts would prove more successful if directed at consumer harm (Information Industry Association, 1997, Ref 19).

The IIA states that broad restrictions in the information industry could have a retarding effect on the economy, and that full economic benefit cannot be realised through the restricted use of information. The author regards this as the primary influence on the IIA's opinion regarding the balance between access to information and privacy concerns.

The IIA holds that public access to information is beneficial to the public and quotes numerous examples of look-up services facilitating individual's searches such as:

- building contractors can be 'scanned' for previous histories before being awarded a contract
- lost persons can be found using look-up services even when in possession of limited information
- addresses can be updated regularly (Information Industry Association, 1997, Ref 19)

It is stated that such searches would take place anyway, look-up services merely make it quicker, more comprehensive and more cost-effective (Information Industry Association, 1997, Ref 19). To the author such an argument seems questionable, since it is the way in which the IIA's services facilitate the methods of personal searches and record matching which is the perceived threat to privacy.

The IIA feels that giving the individual the option of being removed from a database is not practical to most data custodians, an argument also used for dismissing the Use Limitation Principle. Verification of records by individuals also poses a logistical problem, including how to verify the identity of the individual requesting the corrections. They also feel that data such as public records should not be altered by anyone but the responsible authority. It is therefore felt that individuals, at best, be directed to the original source of the record containing incorrect information (Information Industry Association,

1997, Ref 19). The author feels that this in itself presents a problem, since the source of information is not always revealed or cannot be traced back through the database.

The security and access factors in privacy protecting principles is assured by the IIA in that all customers requesting access to a dataset are verified and certified. Criticism can be levelled at the IIA due to the difficulty of deciding uniformly who will be regarded as an authorised user. The economic factor could also have an effect on how many applicants could be granted access.

The IIA sees market forces as a regulating factor in ensuring responsible action by databank holders, and feels that customers will identify irresponsible behaviour and avoid such databank holders who would then be displaced through the competition within the industry (Information Industry Association, 1997, Ref 19).

The IIA feels that US privacy policy is misunderstood particularly by its European counterparts. They hold that while privacy is regarded as a human right in Europe, in the US it is treated as an interest of the individual to be balanced with other social interests. In this climate – created through freedom of expression in the US – individuals are encouraged to protect their privacy interests through their own efforts rather than relying on official regulatory bodies to do so (Information Industry Association, 1997, Ref 19). In the author's view this rather idealistic stance could result in privacy concerns developing into privacy paranoia, if they are indeed not addressed but left to the individual to resolve.

4.2.4 Individual Reference Services Group (IRSG) (US)

The Individual Reference Services Group (ISRG) is an organisation in the United States composed of companies who offer information services including the supply of personal information that is not generally available to the public. It was formed in June 1997 as a result of the Federal Trade Commission's investigation into computerised databases and the use of non-public records.

Subject to growing pressures from concerned parties regarding the protection of privacy in this framework, the ISRG issued a set of self-regulatory principles and announced its' intention of implementing these principles by the end of 1998. The principles are aimed at reducing the risk of misuse of information supplied by an Individual Reference Service (IRS). Self-regulation was seen as the "most effective and efficient way to minimise these risks" (Individual Reference Services Group, 1997, Ref 15). The principles are structured in the form of voluntary restrictions which are imposed on members of the group. Annual audits are performed by professional auditing authorities to assure that principles are complied with (Federal Trade Commission, 1997, Ref 11).

The principles do not facilitate access by individuals to the records held about themselves, and thus do not offer any solution to the problem of inaccurate information contained in personal records (Federal Trade Commission, 1997, Ref 11).

Following are the IRSG principles[12]: (Federal Trade Commission, 1997, Ref 11)

1. Education:

   The IRSG endeavours to educate users and the public about privacy issues arising from the services offered by the group.

2. Reputable sources:

   Before accepting data from sources in government and the private sector it will be established – within reason – that data collection practices of the primary source are understood. When data is acquired from such sources for marketing purposes, it shall only be used for IRS if it is public information, it is specifically permitted by law, or the affected individual was informed of the secondary use at the point of data collection.

[12] See Appendix 4 for the complete set of Individual Reference Services Industry Principles.

3. Accuracy:

Reasonable steps are taken to ensure the accuracy of data. When an individual reports an inaccuracy, it shall – if deemed appropriate – be corrected by the IRSG, or the individual shall be referred to the source of the information. When the inaccuracy is contained in public record information, corrections cannot be made by the IRSG.

4. Public record and publicly available information:

The use of this type of information is not restricted, unless the use is legally prohibited.

5. Distribution of non-public information:

5. (a) Selective and Limited Distribution of Non-Public Information:

The following criteria define the manner of distribution of non-public information:

- it shall be supplied without restrictions to IRS subscribers that comply with the Principles
- the appropriate use for information must be stated by subscribers
- subscribers must agree to confine the use and re-dissemination to such appropriate uses
- subscribers must be identified
- subscribers must qualify as appropriate users by agreeing to terms and conditions regarding the principles.

Each IRS shall endeavour to protect individuals against misuse of non-public information. It shall supply an explanation of what uses and which subscribers of information are deemed appropriate. Before supplying non-public information, the subscriber and the intended use shall undergo a reasonable review. A record of information subscribers, uses, and terms and conditions of supply shall be kept for

three years after termination of service. Reasonable attempts are made to ensure that subscribers use non-public information appropriately, and reasonable mechanisms shall be put in place to remedy abuses of information by subscribers.

5. (b) Commercial and Professional Distribution of Non-Public Information:

Non-public information shall only be supplied to professional and commercial users where the use of the information forms an appropriate part of their business. This excludes information on credit history, financial history, medical records, mother's maiden name identified as such, or similar information; it also excludes information like social security number and birth information unless truncated in an appropriate and industry-consistent manner. Before supplying information, the user shall agree to terms and conditions and to the limitations on use in accordance with the Principles. Protection against misuse shall include the identification of the user as an established professional or commercial entity.

5. (c) General distribution of non-public information:

This shall not knowingly include certain private information (e.g. birth information).

6. Security:

Facilities shall be protected from unauthorised access and confidentiality agreements between employer and employee shall be enforced.

7. Openness:

An information practices policy shall be published and it shall outline the type of information held, the type of sources, the collection method, the type of subscriber to whom it is disclosed, and the types of use.

8. Choice:

Individuals shall be informed of the choices, if any, which can be made in order to limit access or use of their personal information in the data base.

9. Access:

Individuals can upon request be informed about the nature of public information held, and can be provided with non-public information that specifically identifies them.

10. Children:

Non-public information about children shall only be supplied for the purpose of locating missing children.

11. Assurance of compliance:

Annual assurance reviews shall be completed by reasonably qualified independent professional services. Furthermore, information may only be supplied to subscribers who also comply with the principles.

As reported in the FTC review of the ISRG proposal, the ISRG guidelines effectively address the problem of enforcement of guidelines by requiring signatories to comply with them. However, the guidelines do not address the problem of uncontrolled use of public records, which also forms part of privacy concerns. Furthérmore, no requirements for audit trails are specified in the guidelines, which prevents the effective tracing of information use (Federal Trade Commission, 1997, Ref 11).

4.2.5 National Information Infrastructure (US)

In 1994, initiatives were started in the United States to build a National Information Infrastructure (NII), which is intended to allow easier access to information services. To ensure fair information practises, the Privacy Working Group of the Information Infrastructure Task Force was established, with the task of developing a proposal for 'Principles for Providing and Using Personal Information' – intended to define the responsibilities faced by organisations that collect personal data, and thus provide privacy protection to NII users (Electronic Privacy Information Center, 1994, Ref 7).

Following is a summary of the principles for providing and using personal information[13]:

1. Information privacy principle: Individuals are entitled to expect information privacy
2. Information integrity principle: NII participants shall ensure integrity and security of information
3. Information quality principle: information should be timely, accurate, complete and relevant for the intended purpose
4. Acquisition principle: Before collecting personal information, the impact on personal privacy of this collection and the associated use shall be assessed. Only data required for this use shall be kept. It shall be ensured that the data is accurate, up to date, complete and relevant for the intended use.
5. Notice principle: When collecting information directly from individuals, information users shall state the purpose for collection, the expected use, the protection of the data, and any consequences of not supplying the information.
6. Protection principle: Users of personal data must prevent inadmissible disclosures or alterations. This shall be achieved by appropriate managerial and technical controls of the data system.

[13] See Appendix 5 for the complete document as issued by the National Information Infrastructure.

7. Fairness principle: personal information should not be used in ways incongruous with the individual's understanding of its use, unless there is a compelling public interest for such use.
8. Education principle: Information users shall educate themselves, their employees and the public about methods of maintaining information privacy.
9. Awareness principle: It is the responsibility of data subjects to understand the significance of providing personal data. Data subjects must understand primary and secondary uses, protection of the data, any consequences of supplying or refusing data, and rights of redress.
10. Empowerment principle: individuals should be entitled to safeguard their privacy by having access to their personal information, being able to rectify and complete it, and should be able to protect the confidentiality and integrity of the personal information. Individuals are also entitled to their anonymity, when appropriate.
11. Redress principle: if appropriate, individuals have the means of redress if harmed by improper use of the data.

The draft principles were strongly criticised by the Electronic Privacy Information Centre (EPIC).[14] While the final principles are slightly more refined than the draft principles, it would seem that the criticisms still apply. The main criticism lies in the approach taken with regards to the shift in responsibility of privacy protection from the data holders to the data subjects (Electronic Privacy Information Center, 1994, Ref 7). This reflects the general trend in the United States, particularly in the commercial sector, to encourage self regulation, rather than instituting a firm set of principles to be subscribed to. The basic responsibility of privacy protection, according to EPIC's report,

[14] The Electronic Privacy Information Centre (EPIC) is based in Washington DC. "It was established in 1994 to focus public attention on emerging privacy issues relating to the National Information Infrastructure, such as the Clipper Chip, the Digital Telephony proposal, medical record privacy, and the sale of consumer data. ... EPIC... pursues Freedom of Information Act litigation, and conducts policy research on emerging privacy issues" (EPIC, 1994, Ref 7). The reader is referred to the EPIC homepage Ref 5 for a detailed account of their approach to privacy protection.

is to reside with the organisations that collect personal data. The omission of consent by data subjects is also evident.

In 1997, the NII task force issued a report questioning the impact of the privacy principles, in particular on federal data collection (National Information Infrastructure Task Force, 1997, Ref 21). This report also outlines the future options available to the NII in its attempt to provide privacy protection. These are seen as on the one hand, the sectoral approach, and on the other hand the adoption and enforcement of sound privacy protection principles by the federal government. No solutions are given, as the debate around the issue of privacy protection is in the 'options' stage and not the 'solutions' stage (National Information Infrastructure Task Force, 1997, Ref 21).

4.2.6 Information Privacy Principles (Australia)

In Australia, studies revealed that individuals feel that it is the government's obligation to protect the individual from privacy infringements, rather than encouraging self-regulation (Commonwealth of Australia, 1996, Ref 2). While the right of access to and the correction of government-held personal records is regarded as the most fundamental principle of privacy, this right is expanded upon by the Information Privacy Principles, which form part of the Privacy Act of Australia of 1988. For the purpose of this thesis, the author feels that these principles can be included in this discussion of privacy protection guidelines despite the fact that they actually form part of legislation. The following eleven principles are set out in section 14 of the Privacy Act of Australia[15]:

1. Manner and purpose of collection of personal information

   The lawful purpose of collection is to be directly related to the function and activity of the collector, and the collection of the information is directly related to that purpose. No unfair or unlawful means of collection are permitted.

[15] See Appendix 6 for the complete section 14 of the Australian Privacy Act.

2. Solicitation of personal information from individuals concerned

   The individual must be aware of the fact that information is being collected, and the collection of information must be authorised under or required by law. Should the information be disclosed to a third party, this must be made known to the individual.

3. Solicitation of personal information generally

   The collected information must be up to date, relevant and complete. The method of collection must not intrude beyond an unreasonable extent upon the personal affairs of the individual.

4. Storage and security of personal information

   Personal records must be protected against loss, unauthorised access, unauthorised use and modification or disclosure. Should the information be supplied to another person in connection with the provision of a service to the record keeper, everything reasonable must be done by the record keeper to prevent any unauthorised use or disclosure of the information.

5. Information relating to records kept by record keeper

   The record keeper shall enable an individual to ascertain the existence of a personal record, the nature of the personal information, the purpose for holding this information, and what steps can be taken by the individual to access that information. Access to that information may be refused only if this refusal is confirmed by law. The record keeper shall keep an annually updated, publicly available chronicle of what personal records are kept, the purpose for keeping the record, the classes of individuals about whom records are kept, the period for which records are kept, who is entitled to access, and how to access the records.

6. Access to records containing personal information

Individuals are entitled to access personal information, except when refusal of access is based on a provision by law.

7. Alternation of records containing personal information

   Any alterations must be accurate, necessary for the purpose of keeping the data, relevant, complete and not misleading. Should an amendment or alternation be requested by an individual and the record keeper is not able to perform the amendment or alteration, a statement must be attached regarding the correction, deletion or addition requested.

8. Record keeper to check accuracy etc of personal information before use

   The record keeper must ensure that the records are accurate, up-to-date and complete before they are used for their purpose.

9. Personal information only to be used for relevant purposes

10. Limits on use of personal information

    Should information be used for an alternate purpose the affected individual's consent is required. Alternate use is only permitted when it is required in order to decrease threat to life or health of the affected individual or another person, or when it is required by a specific law (such as for the enforcement of criminal law, the protection of public revenue or a law imposing a financial penalty). When such use is required a note stating the secondary use shall be attached to the record. The alternate use must be directly related to the purpose of the initial data collection.

11. Limits on disclosure of personal information

> This is related to principle 2 above, where the individual must be made aware of the fact that information is passed to a third party. Before disclosure, the consent of the individual is required. The disclosure of personal information is limited the same as the use of personal information. The same limits of disclosure shall apply to the third party.

It is envisaged that the implementation of the Information Privacy Principles is elaborated upon by a Code of Practice. Each organisation, industry and profession is encouraged to develop their own Code of Practice to enforce compliance with the guidelines.

Principle 4 is a reaction to the tendency of municipal record holders to outsource or privatise. The problem with municipal and governmental record holders in Australia was commented upon by the Australian Privacy Foundation, revealing that the issue of unauthorised disclosure of government information has reached 'epidemic' proportions as revealed in a detailed report (Privacy International, 1996, Ref 27). This illustrates the difficulty in actually applying legislation relating to the use of personal information. The author further argues that it might illustrate the ineffective implementation of the Information Privacy Principles.

The limitation of the Information Privacy Principles is based on the limitation of the Privacy Act, which only applies to the federal government; the private sector is not affected by the Privacy Act. Principle 4(b) allows some control over the use of governmental records by the private sector in that it extends the compliance with the Information Privacy Principles to the person who receives records for the performance of a service. However, this legal control is very limited as it only applies to data received from the federal government. Various organisations have put forward co-regulatory approaches with respect to public and private sector (Commonwealth of Australia, 1996, Ref 2).

4.3 The Law of Privacy: International

International legislation has been documented extensively (Anderson & McLaughlin, 1993; Curry, 1994; Groom, 1988; Lane, 1985; Lopez & Onsrud, 1994; McCullagh & Robinschon, 1997; Onsrud *et al*, 1994; Peterson, 1994; Rhind, 1992). While not each individual position will be considered for the purpose of this thesis, it is sufficient to say that of the countries mentioned, each shows an individual approach to passing legislation for the protection of privacy.[16] The international context is very significant in the issue of protection of privacy. The transborder flow of personal information is affected by the various policies adopted by the countries involved. Data practises not allowed in one country may be permitted in another, which may give rise to conflicts between trading nations. The gap between European privacy laws and US privacy laws as highlighted by Lopez and Onsrud (1994) could potentially have an effect on the extensive trade between the two.

This thesis does not attempt to give an in-depth analysis of international privacy legislation. However, in order to place the South African privacy law in context, this section on international privacy legislation gives a background on the developments which took place internationally with respect to privacy legislation.

4.3.1 USA

The earliest impact upon American privacy legislation can be traced to Warren & Brandeis' Harvard Law Review article on the right to privacy (1890), which suggested the need for the protection of privacy in the common law.

In 1974 the Privacy Act was passed, to some extent prompted by the Watergate break-in (National Information Infrastructure Task Force, 1997, Ref 21) which caused widespread concern about misuse of government records. The Act controls mainly federal records, and restricts the use of personal

[16] The countries selected for the purpose of this research are amongst the most active in privacy protection. This is not to say that valuable lessons cannot be learnt from other countries. The reader is referred to the Privacy International for a comprehensive discussion of the state of the world's privacy (Privacy International, 1991, Ref 26).

The Act controls mainly federal records, and restricts the use of personal identifiers on records. The Act has been criticised for its various loopholes, including the freedom to change the use of data from the original purpose if the secondary purpose is 'compatible' (EPIC, 1994, Ref 7).

In 1988 the Computer Matching and Privacy Protection Act was passed, with the intention of preventing the creation of large files on individuals. The restriction imposed by the new Act was mainly intended for government. However, geodemographic record matching escapes the control of this act - one does not necessarily need one large database for the creation of a profile of an individual. By accessing publicly available data and combining it using record matching tools, the resulting data profile contains no confidential information as such, but it creates exactly the kind of data profile which concerns individuals (Curry, 1994).

Peterson (1994) comments on the various aspects of the right to privacy in the United States. It is generally regarded as a fundamental right, and has three primary aspects:

1. The state tort law allows a plaintiff to bring action against private citizens or businesses for damages resulting from invasion of privacy.

2. The US Constitution states the individual's right to be free from governmental intrusion into his/her private life. Certain states have expanded on this aspect of the constitution by stating the right to privacy more explicitly.

3. The statutes on the rights to privacy have been developed over the past twenty years, and involve mainly data protection laws relating to fair information practices. They are mainly aimed at government and restrict the government's collection, use, disclosure, retention and disposal of personal information. The individual has a right to

know what type of information is held and updated by the government, and a right to corroborate any such information.

In 1992 almost 1000 bills aimed directly at restricting database activity were passed by the US government. Although this makes the relevant legislature look rather 'piecemeal' (Lopez and Onsrud, 1994), it highlights the need for public agencies to re-evaluate the position taken towards the protection of privacy.

The Alaska Open Records Act of 1990 has been commended for making special reference to electronic information (Dansby, 1992, cited in Anderson, 1992) by advocating the use of electronic data formats and on-line access. Also, it highlights the importance of maintaining a balance between cost recovery, access, and privacy (Anderson & McLaughlin, 1993). Kentucky Open Records Act of 1990 makes special reference to land information, something which is not found in most legislation. It stipulates that while most records can be accessed via the Open Records Act, data held by Kentucky Geological Survey is exempt from this act (Anderson & McLaughlin, 1993). Iowa's Open Records Act of 1989 restricts this access to land information even more so, exerting rigorous control over the release of any geographic computer data (Anderson & McLaughlin, 1993).

4.3.2 Canada

The Canadian Freedom of Information legislation provides for access to non-sensitive, non-confidential records maintained by public agencies. It is aimed at encouraging the *individual* to take the initiative when wanting to access information, rather than *institutions* indiscriminately publishing information for potential interests (Anderson & McLaughlin, 1993).

Data protection laws exist at federal and provincial levels in Ontario and Quebec. These laws encourage the development of fair information practises regarding the collection, use, and disclosure of personal records held by the government.

As a member of the OECD, Canada is bound to comply with the OECD principles of privacy protection.

4.3.3 Australia

The Freedom of Information Act of 1982 allows for access to documents as they exist (Anderson & McLaughlin, 1993). While not reflected in the law, the concern is with the balance between protection of privacy and data distribution. The Australian Senate Standing Committee on Legal and Constitutional Affairs maintains that the circulation of data about identifiable persons does not necessarily constitute an infringement on the right to privacy.

The Privacy Act of 1988 prescribes data protection standards to government practises. It contains specific Information Privacy Principles which are discussed in section 4.2.6. This act offers only limited legislative control over the private sector practises (Commonwealth of Australia, 1996, Ref 2). Attempts are currently underway to extend privacy protection into the private sector.

As a member of the OECD, Australia is expected to comply with their guidelines. However, as stated by Justice Kirby, "Australia lags behind other OECD countries with respect to the implementation of effective laws for the protection of privacy....The protection of privacy is left to the initiatives and consciences of managers" (Groom 1988:163).

4.3.4 UK

The Data Protection Act of 1984 offers protection over personal information to some extent by issuing penalties for the use of this data for purposes other than its explicit purpose (Rhind, 1992). This act applies only to automatically processed data and excludes manually processed data. The Act makes provision for the registration and supervision of data users and computer bureaux. It requires, among other details, the listing of the data collection purpose, who the data will be disclosed to, and data sources. It is up to the

individual to bring civil action against a transgressor. The only criminal offence under the act involves offences related to the registration mentioned above, for instance failure to register or disregard of notices (Lane, 1985).

The UK is not a member of the OECD.

4.3.5 Germany

The *Bundesdatenschutzgesetz* (Federal Data Protection Law) of 1977 controls the electronic and manual processing of all information relating to individuals, with the aim of protecting the privacy of individuals (BDSG 1977). The law applies to all companies processing personal data, and allows the processing of personal data by non-German companies for a German company only under certain conditions.

The law entitles individuals concerned to have access to stored information on them, to corrections thereof, to prevent the use of inaccurate data about them, and to prevent the use of data where the original requirements no longer apply. The law differentiates between the data processing by public authorities, data processing by private establishments for their own purposes, and the commercial data processing by private establishments for others. Commercial establishments are required to store personal information in anonymous form, and are required to store the identifying information separately. This prevents uncontrolled record matching processes. Specific measures are stated for the automatic processing of data and it makes provision for the following practices: admission control, leakage control, storage control, user control, access control, communication control, input control, control of processing on behalf of third parties, transport control, and organisation control (BDSG 1977). A violation of privacy under the German law can only occur if the disclosed private facts identify a particular person (Neethling *et al*, 1996).

Privacy laws in Germany are very strict compared to the UK or the United States, with the *Bundesdatenschutzgesetz* being among the first data protection laws in the world (BSDG 1977). The government takes citizens'

concern with privacy protection very seriously. A result of this was the cancellation of the national Census; the government was unable to alleviate the concern felt by citizens regarding potential misuse of information (Onsrud *et al.*, 1994). However, what came with this cancellation was also the loss of a wealth of information which could have been used to the benefit of the state and its citizens.

4.3.6 Summary

Table 1 gives a brief chronological overview of privacy protection and information access legislation in the USA, Canada, Australia, New Zealand, the UK and Germany, giving an indication of the legislative developments in these countries in the past two decades. Each of the countries mentioned in Table 1 offers an approach to the protection of privacy from which the South African situation can glean valuable information, based on the experiences reported in these countries.

Country/State	***Act***	***Year***	***Description/Limitations***
USA	Privacy Act	1974	Criticised for its loopholes such as ability to change secondary purpose of data use
Germany	Bundesdatenschutzgesetz (Federal Data Protection Law)	1977	strict protection of personal data, referring to both automatically and manually processed data
Australia	Freedom of Information Act	1982	electronic data included
UK	Data Protection Act	1984	excludes manually processed data, stipulates registration of data users
USA	Computer Matching & Privacy Protection Act, Video Privacy Protection Act,	1988	Computer Matching Act has no effect on the computer matching of publicly available databases

Canada	Access to Information Act	1988	refers to both existing documents and electronic data
Australia	Privacy Act	1988	Contains Information Privacy Principles
USA (Iowa)	Open Records Act	1989	strict control over land information access
USA (Alaska)	Open Records Act	1990	special reference to electronic information
USA (Kentucky)	Open Records Act	1990	special protection of land information
USA	Personal Information Privacy Act	1997	prompted to a large extent by data access through the Internet

Table 1

(Sources: Anderson & McLaughlin, 1993; Curry, 1994; Groom, 1988; Lane, 1985; Lopez & Onsrud, 1994; McCullagh & Robinschon, 1997; Onsrud *et al*, 1994; Peterson, 1994; Rhind, 1992)

It seems that the tendency exists on the one hand to allow access to information, in particular state-held information, on the basis of some kind of information access act, and on the other hand to protect information access through some form of privacy protection act. Epstein (1991) sheds light on these processes by pointing out the different values involved in governing the system of information access and distribution (see section 2.3.5). The public values result in legislation such as the Freedom of Information or Open Records act, while the private values lead to legislation such as a Privacy Protection Act.

As stated earlier, no attempts are made here to give an in-depth analysis of international privacy legislation. However, the following section on the law of privacy in South Africa can now be viewed in the international context of privacy legislation.

4.4 The Law of Privacy: South Africa

A brief overview of the structure of South African law will be given, followed by a discussion of relevant cases which have come before the constitutional court, with the focus on court findings and decisions reached regarding the protection of privacy. Common law cases will be discussed, again with the focus on decisions reached regarding the protection of privacy.

4.4.1 Brief overview of South African Law

4.4.1.1 Statute Law

These laws are passed by Parliament. All South African courts are to comply with the statute laws except the Constitutional Court (Barry, 1998).

4.4.1.2 Common Law

This is the general body of law which is developed over the years. These laws are applied by the Supreme Court and the Magistrates' Court. Here the casuistic approach to law comes into effect, where each case is assessed individually and each case contributes to the common law. The lawfulness of a particular action is assessed within its context and the prevailing norms of the community (Barry, 1998).

4.4.1.3 Constitutional Law

In 1996 the Constitution of South Africa was adopted. The constitution is the supreme law of the land. The Constitutional Court has the jurisdiction to rule specific statutes unconstitutional. The principles of the constitution are applied by the Supreme Court to the common law. Due to its 'young' age, the protection of the right to privacy in the constitution is subject to interpretation by the common law (Barry, 1998).

4.4.2 Constitutional Right to Privacy

The constitution contains a bill of rights. It protects the Right to Privacy as a fundamental human right and states the following:

> Section 14: Everyone has the right to privacy, which includes the right not to have -
>
> their person or home searched;
> their property searched;
> their possessions seized; or
> the privacy of their communications infringed.

It also contains the Access to Information Right:

> Section 32: (1) Everyone has the right of access to -
>
> any information held by the state; and
> any information that is held by another person and that is required for the exercise or protection of any rights.
>
> (2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

Corporate entities have the same right to privacy as individuals. This presents concern to certain professionals, who feel that individuals need to be put first in constitutional issues. The South African economy is dominated by a few powerful companies. Critics argue that there is a body of foreign constitutional case law which illustrates the danger of granting constitutional rights to large companies where it concerns individuals - particularly in cases involving freedom of expression and privacy. The legal powers developed by large companies in such cases could compromise the power of the individual (Weekly Mail & Guardian, 1996, Ref 29).

4.4.3 Statutory Law Dealing with Privacy

There is no statutory law dealing with privacy in South Africa. The statutes relating to statistics, census and revenues offer some limited protection against privacy infringements, based on the private nature of the data demanded by the statutes (Fagan pers. com., 1998; Privacy International, 1991, Ref 26).

4.4.4 Common Law

The right to privacy is protected under common law as a natural right. It distinguishes between two infringements on the individual's privacy: firstly, as unlawful intrusion upon their personal privacy, and secondly as unlawful disclosure of private facts about them. Should a violation of this right occur, a person may sue for damages under delict law, apply for an interdict restraining any further intrusion, or lay a charge of criminal *injuria* (Neethling *et al*, 1996a; Erasmus, 1997).

The purpose or justification of the intrusion is considered paramount to any potential conviction. This guides the process of defining the right to privacy in common law, and it means that some intrusion on the personal privacy will be allowed, if the intrusion is judged to be justified. The right to privacy refers to the most personal aspects of a person's life, not to all personal knowledge and experience (Neethling *et al*, 1996a).

The next section will discuss relevant constitutional and common law cases applicable to the principles governing the protection of privacy in South African Law.

4.5 South African Case Law

Case law pertaining to privacy is reviewed and judgements are investigated, in order to elucidate the protection offered to the principles of privacy. Due to the limited amount of cases directly applicable to privacy protection regarding personal data, analogous situations are included in this study. The first section discusses three constitutional cases, while the second section discusses sixteen common law cases, and all cases will be discussed in chronological order. Although the constitutional cases are more influential in the protection of privacy, pre-constitutional cases are still relevant due to the casuistic nature of South African law.

4.5.1 Constitutional Cases

4.5.1.1 Bernstein & Others v Bester & Others 1996

This case relates to a dispute between Mr Bernstein and other partners of a partnership of Chartered Accountants (the applicant) and Mr Bester and other members of the liquidators of Tollgate Holdings Ltd (the respondents). The applicants maintain that the respondents' request for information and documentation on the company infringes on their right to privacy, and request that the respondents are to be prevented by the Constitution from continuing with their examination of the company.

In this case Justice Ackermann gave detailed descriptions and observations regarding the scope of the right to privacy, describing privacy as "amorphous and elusive" (I[65]). He states that the interpretation of each right is always already limited by every right available to other individuals, influenced by societal membership and communities. Such rights of the community can conflict with an individual's personal rights, and leaves the right to privacy as one relating to a truly personal realm. As the individual moves towards activities within the community (such as business and social activity) the personal space diminishes.

Concerns were expressed regarding a tendency to use common law principles when assessing and interpreting *fundamental* rights in the Constitutional Court. It is felt that the Supreme Court should be responsible for working out on a case to case basis a detailed exposition relating to the right to privacy – not the Constitutional Court.

Justice Ackermann expressed the difficulty in defining the term 'right to privacy' due to difficulties in defining the concepts of private life and private sphere. The concept of identity forms part of the explanation of the right to privacy, as it refers to the individual's ability to relate to themselves and to others in a meaningful way (including the private realm and community realm).

South Africa uses a two-stage approach during an inquiry into an alleged invasion of privacy. Firstly, there must be a subjective expectation of privacy, and secondly, this expectation must fall within the realm of reasonableness by society and by the community. In considering infringements of privacy, the Court will deliberate how the information was obtained (for instance whether private information was revealed to the public, whether the information was relinquished, and whether the information was obtained by consent).

After reviewing international legal positions taken by the UK, the US, Canada and Germany with regards to the individual's right to personal privacy, Justice Ackermann states that in South African law, the right of privacy relates:

> "... only to the most personal aspects of a person's existence, and not to every aspect within his/her personal knowledge and experience. The two-stage approach requires, as the first step, a definition of the scope of the relevant right. At this stage already, in defining the right to privacy, it is necessary to recognise that the content of the right is crystallised by mutual limitation. Its scope is already delimited by the right of the community as a whole (including its members)." C[79]

In synthesis, this case influences the legal definition and protection of privacy. It clearly illustrates that the interpretation of privacy included only the most personal and intimate spheres of life. According to this interpretation, when

dealing with social and business issues, the expectation of privacy is diminished as it is affected by the community rights of others.

4.5.1.2 Case & Another v Minister of Safety & Security & Others 1996

This case relates to the possession of indecent or obscene photographic matter, and as an analogous situation can shed light on judgements regarding the protection of privacy. The applicants' had been charged with the possession of indecent or obscene photographic matter as contained in Act 37 of 1967. It was now maintained that the Act is an invasion of privacy, as when such material is kept in the privacy of one's home, the Act requires an intrusion into one's private home that fails the test of justifiability and reasonableness.

Justice Didcott held that any ban on the possession of erotic material kept in the privacy of one's home constitutes an invasion of personal privacy protected by section 13 of the Constitution. This case does not pass the test of reasonableness and justifiability which is used as a guideline when establishing the ruling relating to privacy infringements. Justice Mokgoro departed from the position taken by Justice Didcott regarding the type of material kept in the privacy of one's home, stating that government regulations still have the reach to exercise control over expressive materials.

It was stated that the approach taken by the Court regarding the individual's right to privacy is influenced by the fact that constitutional protection of such a right is new in South Africa. The emphasis on the individual's right to privacy is based on the developments taking place in South African law and practises, illustrating to authority and to citizens that the approach to the protection of such laws and practises has changed.

The analysis of the judgement reveals that under the relatively new constitution, privacy is regarded a right which previously has not received the protection it required. The focus is thus on protecting the privacy of individuals, rather than protecting laws and practices which by their very nature infringe on privacy.

4.5.1.3 State v Motlousi 1996

This criminal trial relates to the gathering of evidence for a criminal trial, and the privacy infringements caused by the unconstitutional methods used in the gathering of the evidence.

The reasoning generated by the Court sheds light on the approaches regarding the right to privacy. The Court held that evidence will not be excluded from a case merely due to unconstitutionality of the evidence. Discretion is exercised by the Court for each specific case in admitting or rejecting particular evidence. This discretion is affected by the nature and extent of the illegality, and by whether the act is intentional or unintentional. Conditions of urgency, emergency and triviality all play a part in deciding on admissibility of seized evidence, as well as the norms of society. It was stated by the Court that should such evidence be obtained by methods breaching the right of privacy, there need to be 'extraordinary excusing circumstances' warranting the admission of this evidence in court.

This case illustrates that the conditions and the context under which an invasion of privacy took place are crucial in deciding on the lawfulness of the action. Again, it brings the argument back to justifiability and reasonableness, as act of privacy invasion can possibly be regarded lawful if the intrusion is justified and reasonable.

4.5.1.4 Summary of Constitutional Cases

In synthesis, the constitutional cases contribute the following to the protection of privacy and the development of accepted practices:

- The interpretation of privacy includes only the most personal and intimate spheres of life. The community rights of other are considered when the interaction is of a social or business nature, in which case the community rights will overrule the individual's right to privacy.
- Privacy is receiving more protection now under the new Constitution than before. This new approach to the protection of privacy implies that certain

laws and practices of the past are questioned and frequently overruled by the individual's right to privacy.

- Justifiability and reasonableness are crucial in deciding on the lawfulness of a privacy infringement. Depending on the circumstance, an invasion of privacy may be regarded lawful when it is justified. However, unconstitutional actions, even when aimed at gathering evidence for a criminal investigation are only tolerated in exceptional circumstances.

4.5.2 Common Law Cases

4.5.2.1 R v R 1954

This case relates to a 'Peeping Tom' or secret watcher situation (the names were kept private). The judge convicted the appellant for the intruding act due the fact that the appellant was fully aware of the infringement of privacy, and that his act was an insult to the victim's dignity.

This case is analogous to personal information privacy infringements in a sense that access was gained to 'information' which an individual intended to keep private, and the perpetrator knew that the information was private. This knowledge and awareness of the intrusion made the act unlawful.

4.5.2.2 O'Keeffe v Argus Printing & Publishing Co Ltd 1954

A photograph of the plaintiff was published in an advertisement without the subject's permission. While the plaintiff consented to the publication of the photograph as illustration in an article, no permission was granted to use this photograph in an advertisement. The Court held that the publication of the photograph presented a violation of the plaintiff's dignity, and interpreted dignity as part of the legally protected personality, and by implication also as part of the right to privacy. This case is regarded as a central case or *locus classicus* of the South African personality right to privacy (Neethling *et al*, 1996).

This case illustrates the Court's application of a Use Limitation Principle with respect to personal information. While no reference is made to the OECD Use Limitation Principle, this judgement is a practical application of the principle, which states that personal information should not be used for secondary purposes without the consent of the data subject.

4.5.2.3 Kidson v SA Associated Newspapers Ltd 1957

This case relates to a situation where permission was given to publish a personal photograph in an illustrative article in a nursing journal, but not to be used in a nation-wide fund raising campaign article with the heading '97 Lonely Nurses Want Boy Friends'. An action was instituted by the three subjects of the photograph (two of whom were engaged, and one married) on the grounds of defamation and *injuria* (an invasion of their privacy and dignity). Only in the case of the married nurse did the case of *injuria* succeed.

Regarding the relevance to privacy protection guidelines, this case again relates to the Use Limitation principle as outlined in the previous case. It also relates to data quality, in a sense that the information published was not an accurate reflection of the subjects, which was a factor in the judgement of the actions as an invasion of their privacy.

4.5.2.4 Gosschalk v Rossouw 1966

This is a leading case in establishing whether violation of an individual's privacy in public interest is justified (Neethling *et al*, 1995). The Court held that it is the function of the Court to enforce Parliament's will and thus give the police the statutory capacity to interrogate people. In post-constitutional case law, this assertion is now overruled by the Constitution of 1996 protecting privacy as a fundamental human right. Now it is felt by the Court that reasonableness has to be used as a guideline to judge where infringement of privacy is warranted in public interest.

This case shows the approach taken to privacy protection in pre-constitutional cases. In the new approach adopted with respect to the protection of privacy,

justifiability and reasonableness are keywords in deciding on the lawfulness of an invasion of privacy.

4.5.2.5 State v A and Another 1971

This case involved the listening in by use of a recording device by a private investigator hired to investigate a suspected case of infidelity. It led the Court to conclude that the invasion of privacy by a wrongful act does not necessarily constitute *crimen injuria*; an actual impairment to dignity is seen as an essential element. The Court considered the fact that the intention of the data collection (by listening in) was not to affect the appellant's dignity, but to shed light on an unlawful act. The prevailing norms of public opinion were respected by the Court.

When analysing the judgement of this case, the author contends that under today's constitution the case may be decided differently, as the justification for the privacy infringement would be viewed under different light.

4.5.2.6 Mr and Mrs 'X' v Rhodesia Printing and Publishing Co Ltd 1974

This case relates to the applicants applying for an interdict against a publishing company stopping them from revealing names in the publication of facts surrounding a custody battle. It is argued that publishing the name of the parents or the child could potentially infringe on the parents' or the child's right to privacy. The application led to the judge ordering in camera hearings and issuing an interdict preventing the publishing firm from stating the names of the persons involved in the custody battle.

The relevance of this case to the issue of privacy protection is clear, in that it supports the notion that individuals should be able to determine the destiny of private facts about themselves. In this case this extended to the protection of the privacy of a child.

4.5.2.7 Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977

This case involved the University of Pretoria claiming infringement of their privacy through a film produced by Tommie Meyer Films (Edms) Bpk which related the story of a racial incident in student rugby circles. The Court held that a university is impersonal in a sense that it cannot suffer personal injury of the *corpus* (physical integrity), *fama* (good name) or *dignitas* (dignity). Such acts are only experienced by human beings, and the infringement of privacy is part of such act. The same follows for personality rights, which are also not available to institutions such as universities.

This case sheds light on the approach taken with respect to the protection of institution's information. The right to privacy does not form part of an institution's right protected by the law.

4.5.2.8 Reid-Daly v Hichmann and Others 1981

This case relates to the secret installation of an electronic transmitting device and receiving system in the plaintiff's office for the purpose of intercepting and monitoring the plaintiff's personal and official telephone conversations, to the removal and copying of personal information from the plaintiff's office, and to the plaintiff's surveillance. It was argued that these actions constitute attack on the plaintiff's *dignitas* and an invasion of his privacy which have injured him in his dignity and reputation.

The Court held that the planting of a listening device in an apartment does in itself amount to an impairment of the occupier's *dignitas*, and that the copying of personal documents constitutes an *injuria*. The fact that the plaintiff was an army officer and that the intrusions were made by other military authorities did not affect this conclusion, as there was no military obligation to perform such insults to a person's dignity. It was found that whatever military directive these acts were performed under, they are not relevant to the case at hand.

Again, this highlights the importance of justifiability and reasonableness as a consideration in the judgement regarding invasions of privacy.

4.5.2.9 State v Bailey 1981

This case relates to a medical practitioner refusing to furnish particulars on a questionnaire for the Department of Statistics. The defence claimed that such action interfered with his right to privacy as the requested information relates to his private affairs. The defence was not upheld, and the Court held that for the census benefit and in compliance with the Statistics Act the medical practitioner was required to complete the questionnaire. The information requested in the questionnaire related to the activities of the general practice.

This case shows that the nature of the information plays a crucial role in deciding on issues surrounding privacy. As in the constitutional case of Bernstein and Others v Bester and Others, the business aspect of the requested information removes the expectation of privacy in this case, and the right to privacy diminishes.

4.5.2.10 Culverwell v Beira 1992

This case relates to the applicant demanding the handing over and destroying of compromising and intimate photographs of her taken by the respondent during a period when the two were engaged in romantic relationship. The Court found that the owner of the photograph is in fact the respondent, since he paid for the film and the developing. The termination of their relationship did not entitle the appellant to the return of the photographs due to their intimate and private nature. The Court further held that the respondent was also entitled to make copies of his photographs, as long as they are not used for publishing.

This case presents an appropriate analogous situation for a comparison to databanks, although the focus rests more on ownership of data than on privacy infringement. In this case the Court found that despite the fact that the appellant was the subject of a set of photographs, she had no right over them,

had no right to demand the negatives or the destruction thereof. The person who had bought the film and had paid for development of the photographs was found to be the rightful owner of the photographs and the only person to decide on the circumstance surrounding the photographs. If the photographs can be equated to data, this would imply that the data subject does not have say over the data, but the data owner. This is clearly limited by law as far as the use of the photographs/data goes, in a sense that it cannot be used for unlawful publication (for instance for advertising if the data subject has not permitted such use).

4.5.2.11 Jansen van Vuuren and Another 1993

This case relates to a breach of the right to privacy by a medical practitioner who shared his knowledge of a patient being infected with the AIDS virus with two other persons, despite the fact that the patient expressly requested the medical practitioner to keep this information private. As a result of this public disclosure of private facts the plaintiff claimed he has suffered an invasion of his rights of personality and his right to privacy. The Court found that the defendant wrongfully and unlawfully disclosed the patient's health condition to third parties.

Judge Harms states here that privacy is regarded a 'real right', but is more accurately described as a personality right. The right to privacy is in this case also protected by the Hippocratic Oath which medical practitioners are required to take. In weighing up conflicting interests, the Court came to the conclusion that in this case the private information was not of public interest, i.e. that the medical practitioner was not acting under his obligations to society.

In response to the defence, Judge Harms continued to discuss the lawfulness of publishing private information and states a test reported by Burchell Principles of Delict at 180 in the context of defamation: 'It is lawful to publish ... a statement in the discharge of a duty or the exercise of a right to a person who has a corresponding right or duty to receive the information. Even if a right or duty to publish material and a corresponding duty or right to receive it

does not exist, it is sufficient if the publisher had a legitimate interest in publishing the material and the publishee had a legitimate interest in receiving the material.' This duty is twofold and refers to one of legal duty (for instance where a medical practitioner is required to testify before a court of law), and a social or moral duty (see Hague v Williams, where a medical practitioner informed an insurance company of a prospective client's heart problem). In other words, the right to disclose information does not have to exist when there is a justifiable interest in the information by the recipient.

4.5.2.12 Financial Mail (Pty) Ltd and Others v Sage Holdings 1993

The publishers of the said magazine had gained access to information by means of tape recording telephone conversations between the Respondent's directors and board members, and the appellant wanted to use this information for another purpose, that of publication. In this case the court held that companies (*juristic* persons) have the same right to privacy as do individuals.

This case is regarded as a principal case in South African privacy law (Fagan, 1998). The Court held that there was a need to ascertain the public interest of being informed of facts in question. If that was found to be the case, the publication should be permitted. The manner in which the information was obtained would not necessarily mean that the information cannot be used by the appellant, as the public good in this case may prevail over privacy. The Court held that in this case the public good found no benefit from the publication and therefore did not allow it, but rather found the unlawful intrusion by means of recordings to be significant. Particular attention was drawn to the distinction between 'interesting to the public' and 'in public interest', which often leads to confusion in the media industry similar to one of financial interest of the publisher v the public interest.

In his exposition of privacy, Justice Corbett held that breach of privacy can occur in two ways: (a) by an unlawful intrusion upon the personal privacy of another, or (b) by unlawful disclosure of private facts about a person. In

judgement the contemporary *boni mores* and the sense of justice of the community as perceived by the Court are taken into consideration.

The relevance to data banks is shown in this case by the similarity in conflict of interest: the interests of the databank holder – when related to the economical factor (the value of data and information) – can be in conflict with the interests of the data subject.

4.5.2.13 State v Hammer and Others 1994

This case relates to a prisoner handing a letter addressed to his mother to a guard for posting, and the guard proceeded to read the letter and bring the contents to the attention of the authorities. The Court held that the evidence would not be taken into consideration, and it was rejected based on the unlawful means of obtaining it. The prison guard was found guilty of an *injuria* to the prisoner.

4.5.2.14 Motor Industry Fund Administrators and Another v Janit and Another 1994

In this case the applicant was seeking an order preventing the respondent from using as evidence in legal proceedings the contents of tape recordings of meetings of the applicant's board of directors and from disclosing the contents and nature of such recordings to any other person. Secret tape recordings of his previous employers' board meetings were obtained by the respondent from a disgruntled employee. The Court held that the recordings were not to be used as evidence, and further held that the respondent must comply with non-disclosure to any other parties. The respondent was required to disclose all names of parties who had already become privy to the information on the recordings, and to submit all copies of the recordings to the applicant's attorney.

The judgement here was based on the fact that the recordings were obtained secretly, and that the subjects were not informed. The Court held that it was

an act of unlawful intrusion of privacy by means of unlawful access to information. The Court held that

> "in demarcating the boundary between lawfulness and unlawfulness of the intrusion/publication, the Court must have regard to the particular facts of the case and judge them in the light of contemporary *boni mores* or the genuine sense of justice of the community".

This case clearly illustrates and supports the collection limitation principle, which states that collection of information must be lawful, fair, and with the consent of the data subject.

4.5.2.15 National Media Ltd and Another v Jooste 1996

This appeal case relates to the breach of an agreement concerning the timing and the content of article in a newspaper, where the newspaper published certain facts and photographs without complying with the conditions laid down in the agreement between the two parties. More specifically, an interview regarding her relationship with a prominent person was granted by the respondent to the appellant under the condition that the resultant article photographs would be subject to her approval. The present case forms an appeal to a decision to award the respondent damages for the invasion of her privacy (see Jooste v National Media Ltd and Another 1994 (2) SA 634). It was then argued that the respondent had already decided to make public certain private facts about the relationship, and that therefore her expectation of privacy was not reasonable. The Court held that this submission was unsound since her decision to go public with certain private facts was based on an agreement limiting the conditions for the publication. The Court further held that the general sense of justice of the community required that such an agreement need to be upheld. The publication was regarded as wrongful in a sense that it did not comply with the agreement; should the publication have taken place in compliance with the agreement, it would *not* have been wrongful for reasons such as lack of will to preserve privacy. The appeal by National Media Ltd was dismissed.

Justice Harms noted how the right to privacy included the ability to determine the destiny of private facts, when, where and under what conditions private facts were made public. The Court described privacy as a

> "voluntary and temporary withdrawal of a person from the general society through physical and psychological means, either in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity or reserve".

This case demonstrates the court's application and support of the purpose specification principle, which states that data should only be used for the purpose specified upon data collection. The individual participation principle was overruled by the publishing firm, as it did not allow the individual to determine the existence and conditions of publication. In analysis, the Court clearly upheld these two principles by dismissing the appeal by the publishing firm and ruling in favour of the respondent.

4.5.2.16 C v Minister of Correctional Services 1996

This case involves the invasion of privacy of a prisoner subjected to having an HIV blood sample drawn by a prison official, without the possibility of informed consent regarding the blood test and in the presence of other prisoners. The Court held that there could only be consent if the person appreciated and understood what the object and purpose of the test was. The Court further held that the prisoner did not have adequate privacy awarded when reflecting on the decision regarding the taking of the test, which constituted an invasion of his rights of personality, more specifically of this right of privacy. Despite this finding, it was also stressed that the privacy of the individual is not absolutely inviolable in law.

Injuria is only the case when there was proven intent to violate the right to privacy; "*Injuria* is the wrongful and intentional infringement of an interest of personality" (at 305 D). In this case, although the infringement of privacy was objectively unjustifiable, no intent of invasion of privacy can be proven. The Court stressed the fact that the absence of knowledge of or consciousness of

the wrongfulness of an act does not eliminate the possibility of unlawfulness of the act.

This case shows the application of the collection limitation principle, and it highlights the importance of informed consent when data is collected about an individual, in this case it was medical data. Informed consent means to fully appreciate and understand the object and purpose of the data collection, which can then in turn enable an individual to make full use of her fundamental right to self-determination.

4.5.2.17 Summary of Common Law Cases

In synthesis of the sixteen cases investigated above, the following contributions to the common law can be extracted:

- Individuals are supported in their ability to determine the existence of personal data and the destiny thereof.
- Justifiability and reasonableness (the *boni mores* of the community) are crucial in deciding on the lawfulness of a privacy infringement.
- The Court applies concepts reflected in the use limitation principle, the collection limitation principle, the purpose specification principle, and the individual participation principle.
- Public interest versus private interest in under consideration in the judgements. However, the focus lies on the individual's rights to privacy.

The following chapter analyses the influence of the case law reviewed in this section with respect to data collection methods and information use.

Chapter 5: Analysis

5.1 Introduction

This chapter analyses the legal influences on privacy protection guidelines as imposed by the South African law, and as revealed in the previous chapter. The effect of this on data use and data collection methods is studied. Ownership issues are briefly discussed. The legal implications of privacy expectations are discussed in the way they influence the lawful use of private data. Before formulating a set of privacy protection guidelines for GIS in South Africa, the objectives to be met by such guidelines are elaborated upon.

5.2 Legal Influences

Before constructing a set of guidelines for the protection of privacy, the influence of the legal aspects described in the previous chapter will be discussed. What follows is a summary of legal factors which have direct bearing on how information can or cannot be used, and which can affect the formulation of guidelines for privacy protection.

5.2.1 GIS data-gathering

Data gathering methods for GIS are clearly influenced by the law. Secret data gathering is found to be unlawful in almost all cases. An exception is for instance the criminal case where unlawfully obtained evidence is admitted due to the value of the information to public interest (see State v Motlousi 1996). This means that any secretly obtained data cannot be used for commercial purposes. Bugging, listening in, secretly taping, the secret copying of private documents are acts which constitute *iniuria* and imply an impairment of *dignitas* (see Motor Industry Fund Administrators (Pty) Ltd and Another v Janit and Another 1994). Modern technology may now require the inclusion of surveillance techniques such as satellite and remote sensing techniques in the list of secret data gathering methods, depending on where such data is made available.

Furthermore, it was found that subjects need to be informed of the data gathering process in order for the data gathering process to be lawful (see for instance Motor Industry Fund Administrators (Pty) Ltd and Another v Janit and Another 1994).

Subjects do not only have to be informed of the data gathering process, but they also have to be able to give informed consent (see for instance C v Minister of Correctional Services 1996). This implies full understanding on behalf of the subject of the data gathering process and the data use. It also suggests that once subjects are informed of the intention for data gathering (i.e. of the use the data will be put to), this use cannot change once the data is gathered, even if the secondary use is within the domain of the law.

5.2.2 Data use

The use of data is limited by the law. Private data can only be used for the purpose stated and individuals have recourse to object to any other use of the private data.

It is stated that even when consent is given to the publication of certain private facts, the consent is given to a *particular* publication, and not to *any* publication of that information; in cases where photographs were used in publications for purposes other than initially specified by the subject, the publishers were found to act unlawfully (see for instance O'Keefe v Argus Printing & Publishing Co Ltd 1954, Kidson v SA Associated Newspapers Ltd 1957). Data use can also be limited by certain conditions (see for instance National Media Ltd and Another v Jooste 1996).

Neethling *et al* (1996) makes specific note of the fact that common law is very limited with regards to mass publication of private facts (not intended for publication), since mass media has only in the past few decades become an issue in the spread of information. However, in general it is held that mass publication of private information is always wrongful. Private data cannot be

used by a third party. Disclosure of private data to a third party constitutes *crimen iniuria*.

5.2.3 Ownership of data[17]

In the case of Culverwell v Beira 1992 it was found that the data subject does not have the right to decide over the destiny of the data, but the data owner - bearing in mind that the data owner is limited in his right over the data in a sense that he is only able to use the data within the confines of the law (i.e. he is not entitled to publish the data as that would infringe on the data subject's right to privacy). However, it is interesting to note that the data subject in this case was *not* entitled to decide over the existence of the photographs which by virtue of their intimate and private nature may have been construed as invasive of her privacy. Further case law is required to interpret the effect this ruling may have on the ability of data subjects to determine the existence of their private data in a data bank.

5.2.4 Expectations of privacy

The individual's expectation of privacy is important when assessing the lawfulness of use of private data. Certain relationships are regarded relationships of confidentiality and provide the individual with an expectation of privacy and an expectation of non-disclosure of private data to third parties. Any information revealed within the domain of this relationship is regarded private and protected as it is intended only for specific persons. Any disclosure of such information to third parties or the publication thereof is regarded unlawful and constitutes a breach of privacy (see for instance Jansen van Vuuren v Kruger 1993). A confidential relationship exists between doctor and patient, legal representative and client, banker and client, priest and penitent, and public servant and subject.

[17] Ownership of data (including intellectual property and copyright) are in themselves extensive and controversial topics. While no attempts are made here to include these issues, ownership of data also affects privacy and a subsection on the ownership of data is warranted here.

5.2.5 Limitations of the right to privacy

The protection of personality rights and the emphasis on the individual's right to privacy has become an important issue in South African law (see Case & Another v Minister of Safety & Security & Others 1996). However, this right to privacy relates to the most personal aspect of a person's life.

For the use of private data to be regarded unlawful, certain conditions are considered:

Firstly, it has to be proven that the individual had a certain expectation of privacy. This suggests that if an individual makes public certain private information, the expectation of privacy is lost to a certain extent. However, this depends on the extent of publication.

Secondly, the purpose of or the *justification* for the intrusion is relevant. In the case of the publication of private data, if it can be proven that the publication is of public interest and to the benefit of the public, the publication will not be regarded unlawful. Justification includes

(a) necessity (Neethling's example: where a person enters a private residence to escape from violent rioters and infringes on the privacy of the resident out of necessity)
(b) private defence (where a spouse obtains information about an adulterous relationship)
(c) public interest (see Gosschalk v Rossouw 1966)
(d) voluntary consent (see National Media Ltd & Another v Jooste1996)
(e) defamation (where in certain cases private facts need to be revealed)

Justification for the violation of privacy must remain within the realm of what is necessary.

Thirdly, intent is relevant. If the data in question was obtained by coincidence (for instance Neethling's examples where a person by chance overhears a conversation nearby, or a person by chance catches a glimpse of the happenings in another's bedroom) then the surrounding circumstances will prevent the 'infringement' from being regarded unlawful as there was no

intent. Before liability can be established, it has to be proven that the perpetrator was aware of the wrongfulness of the act (Neethling *et al*, 1996).

In the case of disclosure of certain private facts the possibility of identification of an *individual* influences the lawfulness of disclosure. In discussing disclosure or revelation, Neethling *et al* (1996) points out that "... in all of these instances the question of an infringement of privacy arises only if the plaintiff is identified with the disclosed facts. If this element of identification is lacking, the disclosure does not relate to a specific person in his state of privacy." (*ibid.*: 248). This is of particular interest to GIS, where the geographical element makes the information more sensitive, as it facilitates the identification of one particular *individual*. It is also inferred that in cases of identifying information, the principles of the right to privacy extend to the protection of personal information.

It is important to note that privacy infringement can only be the case where outsiders are acquainted with personal facts *contrary* to the determination and will of the individual whose right is infringed (Neethling *et al*, 1996). This has implications for data banks holding general demographic data, where individuals cannot claim privacy infringement.

5.3 Objectives of Guidelines

The effect of privacy protection guidelines depends to a large extent on their availability and implementation. Based on the reported implementation and synthesis of researched privacy protection guidelines, it can be concluded that the following constitute a reasonable set of objectives for guidelines: (Commonwealth of Australia, 1996, Ref 2; EPIC, 1994, Ref 7)

- guidelines should have a regulating effect on the use of information
- guidelines should regulate the actions associated with the use of information, for instance the comparison of information about identifiable persons
- guidelines should be publicly available

- guidelines should provide a policy framework
- guidelines should provide data holders and the public with a mechanism to assess privacy implications of their actions
- the compliance with guidelines should be compulsory for members of a given association
- guidelines should be non-technical and unambiguous

Wacks (1980) suggests a number of preventative measures which can be taken to prevent the misuse of personal information[18]; they can be divided into the following five categories:

1. Security
2. Type of Information
3. Personnel
4. Regulation
5. Access

Wacks (ibid.) offers realistic limitations to each of these categories, and maintains that the adoption of the suggested preventative measures can assist in avoiding the misuse of personal information. Privacy protection guidelines should offer solutions to the preventative measures listed above.

Self-regulation is an approach offered by various associations as a solution to the privacy problem, instead of privacy protection guidelines.[19] The effectiveness of self-regulation without the implementation of privacy protection policies has been questioned (National Information Infrastructure Task Force, 1997, Ref 21; Federal Trade Commission, 1997, Ref 11). "Critics point to one central weakness with this approach: the lack of either incentive or mechanism for enforcement" (Federal Trade Commission, 1997, Ref 11:292). Moreover, the difficulty of upholding self-regulation in the industry once public attention declines and the difficulty of controlling non-adherence to self-regulation also raise the question of whether self-regulation can offer

[18] See Wacks (1980) *The Protection of Privacy* for a detailed account on the solutions offered for the prevention of privacy infringements through the use of computers.
[19] See for instance the Individual Reference Services Group or the Direct Marketing Association of US. The subscription to privacy guidelines by DMA members is voluntary which has lead some critics to question the ability of enforcement (EPIC, 1994, Ref 7).

appropriate safeguards against privacy infringements and create the need for regulation through policy.

Guidelines should be stated in such a way that they can be practically implemented, i.e. there should be no possibility for data controllers to escape the guidelines due to logistical or practical difficulties – something one might call the 'practicality obstacle'. This implies that the guidelines should be stated in an all-inclusive way, rather than too specifically. An example would be the phrasing of Article 10(3) of the European Union's directive (see Section 4.1.2): the phrase 'categories of recipients' is included in the guidelines, which makes it more all-inclusive and more general; data controllers can more readily be expected to supply the categories of recipients of data rather than the individual recipients. This helps to eliminate non-compliance with the guidelines.

5.4 Privacy Protection Guidelines for GIS

Based on the synthesis of the research and analysis presented in this paper, the research of existing privacy protection guidelines in Section 4.2, the research of legal influences on the protection of privacy offered by the South African courts as presented in Section 4.4, 4.5 and 5.2, the following privacy protection guidelines are proposed for GIS in South Africa, the foundation of which are the OECD guidelines:

1. **Collection Limitation**: There should be limits to the collection of personal data. Personal data collection should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality**: Personal data should be relevant to the purpose for which it is to be used. The data should be necessary for this purpose, should be accurate, complete and kept up to date.
3. **Purpose Specification**: The purposes for which the data is to be used should be specified upon data collection. The subsequent use

should be limited to these purposes or purposes that are compatible with the stated purposes.

4. **Use Limitation**: Personal data should not be used for secondary purposes without the consent of the data subject or the authority of the law.

5. **Security Safeguard**: Personal data should be protected by the data controller against risks such as loss, modification, disclosure and unauthorised access.

6. **Openness**: A general policy of openness about developments, practices and policies with respect to personal data should prevail.

7. **Individual Participation**: Individuals should be able to ascertain and determine the existence of data about them, to inspect and to rectify such data.

8. **Accountability**: The data controllers should be held accountable for conforming with these guidelines.

9. **Education**: Data controllers should be committed to educating data subjects and data users about the implications of the use of personal data, and the risks of privacy infringements. To facilitate this education process, the privacy protection guidelines should be publicly available and actively distributed.

10. **Minimisation of personal data collection and storage**: data controllers should be committed to assessing the need for collecting and storing personal information *prior* to data collection and only do so when alternative options are not available.

Guidelines 1 to 8 are the basic principles of the OECD privacy protection guidelines. These guidelines form the core of most privacy protection guidelines reviewed during the course of this study. Based on the international experience researched it was concluded that these core guidelines effectively address the objectives proposed in section 5.2., and are thus also appropriate for the South African context.

Guideline 9 – education - appears explicitly in both the ISRG guidelines and in the NII guidelines; it seems to form part of the self-regulation approach. The education principle is linked to the principles of openness and individual participation. It is proposed that a conscious commitment to the education of the public and the information industry with respect to privacy issues will raise awareness. This increased awareness can assist in the avoidance of misuse of personal data, and is thus regarded as a core component of effective privacy protection guidelines.

Guideline 10 is based on a specific recommendation made by the interim report of Privacy International[20] in 1991.[21] None of the researched guidelines devote a distinct principle to this purpose. As suggested by Wacks (1980) the prevention of misuse of personal information is a significant step towards solving the privacy problem; it is thus submitted that by reducing personal data collection and storage to a minimum, the misuse of personal data can be decreased. An example would be the use of census data in an anonymous form rather than using personal data with a high privacy infringing potential. Clearly the application in question is instrumental for the type of data required. While this aspect is also addressed by the collection guideline and the data quality guideline, it is assumed that special reference in a discrete guideline will underline the importance of prevention.

---

[20] Privacy International (PI) is a global coalition based in the UK. "Privacy International has been established to protect the peace, dignity and individual rights of people throughout the world. It seeks to raise awareness of violations of privacy rights, and to establish limits to the unreasonable surveillance of individuals. Privacy International is an independent, non-profit and non-partisan organisations that supports the principles of the Universal Declaration of Human Rights and the privacy principles of the Council of Europe and the OECD" (Privacy International, 1991, Ref 26). The approach by PI is unique in that it attempts to also associate with countries that do not provide privacy protection; this association is aimed at promoting expertise and privacy protection pressures.

[21] PI's Special Report on New Zealand offers a critical assessment of the state of privacy protection in New Zealand and detailed recommendations as to its improvement are submitted (Privacy International, 1991, Ref 26).

Chapter 6: Summary of Conclusions and Recommendations

6.1 Introduction

The capacity of GIS allows data operations that are potentially threatening to an individual's personal privacy. Thus, GIS data holders run the risk of infringing on personal privacy. There are methods which can be employed to minimise this risk, and the adherence to privacy protection guidelines is one such method. This thesis researched the issues surrounding privacy protection by investigating the international context of privacy protection and by reviewing South African legislation relating to privacy. The aim was to develop a set of privacy protection guidelines for the South African GIS community.

6.2 Findings

In developing a set of privacy protection guidelines, the international body of research regarding privacy protection was reviewed. The work done by numerous privacy proponents in Europe, the United States and Australia was studied focussing on the objectives of privacy protection guidelines. The privacy protection guidelines, also called fair information practises, of six organisations were reviewed. The most salient features of the guidelines address collection and use limitation, data quality and the individual's right to participation. This is contrasted by the commercial information industry which focuses predominantly on self-regulation as a privacy protecting mechanism. While self-regulation in combination with privacy protection guidelines can be effective in ensuring fair information practices, self-regulation as the primary privacy protecting policy leaves the individual's privacy vulnerable to abuse.

In order to assess the suitability of guidelines for the South African GIS community, South African privacy legislation was examined. In South Africa, privacy is a fundamental human right. It has become evident in the course of this research that while the right is protected by the constitution and by

common law, there is need for accurate and precise legislation protecting privacy with respect to personal information systems. While privacy protection guidelines such as the guidelines proposed in this study can form the basis for a code of practice, they do not replace the need for legislation.

The South African case law pertaining to privacy was reviewed in this study. However, due to the limited amount of cases directly applicable to the study, analogous cases had to be included. It was found that legislation has an influence on the data gathering method, the use of data, and the ownership of data. The study of case law also revealed that the expectation of privacy is a crucial element in the assessment of privacy infringements. While it is felt that the reviewed case law is sufficient to elucidate its bearing on privacy protection guidelines, it is recommended that for further study the United Kingdom case law is reviewed, as in South African law a particular status is granted to British law (Fagan, 1998).

The GIS community in South Africa needs a specific set of guidelines generated to ensure that data practises do not infringe on personal privacy. The guidelines proposed in this thesis are based to a large extent on the OECD guidelines; this was also reflected in the reviewed guidelines, and in the author's observations it leads to conclude that the OECD guidelines can be regarded as a standard in privacy protection guidelines. However, this thesis proposes *education* as one of the guidelines; it is presumed that through increased education the awareness of privacy issues will be raised and the problem will be addressed more readily. Furthermore, the *minimisation* of personal data collection and storage is proposed as a guideline; this is based on a 'prevention is better than cure' type of motivation, where the need for privacy protection only exists in data bases which store personal information - thus, minimisation of personal data storage prevents this need.

The generation of guidelines needs to be accompanied by methods of enforcing adherence to the guidelines, without which they become ineffective. There is thus a need for a professional body to be developed. It is envisaged that such a professional body would generate information policies based on the type of privacy protection guidelines proposed in this study.

6.3 Conclusion

The current decade has witnessed fundamental changes in South Africa, one being the creation of the South African constitution which was adopted in 1996. In Case and Another v Minister of Safety and Security and Others, these central changes with respect to the protection of privacy are reflected:

> "[100] The emphasis with which Didcott J expresses himself with regard to the individual's right to privacy has to be seen against the backdrop of our history and the fact that constitutional protection of this right is new in this country. It is a right which, in common with others, was violated often with impunity by the Legislature and the executive. Such emphasis is therefore necessary, particularly in this period when South African society is still grappling with the process of purging itself of those laws and practices from our past which do not fit in with the values which underpin the Constitution - if only to remind both authority and citizen that the rules of the game have changed."

When researching the issue surrounding privacy protection, it became apparent that privacy protection is not as topical in South Africa as it is in Europe, Australasia and America. In the author's view, the more moderate pace of technological development in South Africa with respect to information systems is seen as the reason for this. While the advanced states are adapting to the global information super-highway, South Africa has not reached the stage of being a large scale information society. The contrast in privacy protection between advanced and less advanced countries needs to be reduced, in order to facilitate the development of a 'Global Information Society'.

Fortunately, this also means that South Africa has not yet had to deal with privacy concerns to the extent that Europe, Australia and America has. This gives the development of privacy protection guidelines and legislation in South Africa an advantage as it can draw on the expertise and the experience

offered by international authorities in the field. With the required infrastructure currently being developed, South Africa can expand into an information society with the aid of privacy protection guidelines and hopefully curtail the privacy problem before it becomes unmanageable.

Bibliography

Books and Journals

Alpert S. and Haynes K.E. (1994) *Privacy and the Intersection of Geographical Information and Intelligent Transportation Systems.* In Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

Anderson R.I. (1992). *Access and Privacy of Distributed Land Related Information.* M.Sc.E. thesis, Department of Surveying Engineering Technical Report No. 161, University of New Brunswick, Fredericton, New Brunswick, Canada, 166 pp.

Anderson R. & McLaughlin J. (1993) *Access and Privacy of Distribution Land Related Information.* In The Australian Surveyor. Vol. 38 No 2. pg. 120-131.

Barry, M. (1998). Unpublished Lecture Notes in Land Law. Department of Geomatics, University of Cape Town.

Curry M.R. (1994) *In Plain And Open View: Geographic Information Systems And The Problem Of Privacy.* in Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe,AZ,October 29-31.

Dansby H. B. (1991) *Informational Privacy and GIS.* In Annual Conference of the URISA. San Francisco, California. URISA 4: 18-28.

Dansby H.B. (1992) *Survey and Analysis of State GIS Law*, GIS Law Volume 1, No 1, pg 7-13.

Epstein E. F. (1991) *Legal Aspects of GIS.* In Geographic Information Systems. Ed. D.J. Maguire, M.F. Goodchild and D.W. Rhind. Longman Scientific & Technical. London.

Fisher J.D., Bell P.A. & Baum, A. (1984) *Environmental Psychology (2nd Edition).* Holt, Rinehart and Winson. New York.

Flaherty D.H. (1979) *Privacy and Government Data Banks.* Mansell, London.

Flaherty D.H. (1994) *Privacy Protection in Geographic Information Systems: Alternative Protection Scenarios* . in Proceedings of the Conference on

Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

Gesellschaft für Datenschutz und Datensicherung e.V., Bonn (ed) (1977) *Law on Protection against the Misuse of Personal Data in Data Processing (Bundesdatenschutzgesetz – BDSG).* Fritz Knapp Verlag, Frankfurt am Main.

Groom G.G.D. (1988) *The Land Information Revolution.* In The Australian Surveyor, Vol. 34, No 2, pg. 153-170.

Hutchinson D. (ed) (1974) *Wille's Principles of South African Law (8th ed.).* Juta & Company Ltd. Kenwyn.

Laudon K.C. & Laudon J.P. (1998). *Management Information Systems (5th ed.).* Prentice Hall, New Jersey.

Lane, V.P. (1985) *Security of Computer Based Information Systems.* Macmillan Education Ltd. London.

Lopez, X. and Onsrud H.J. (1994) Information Privacy and the Use of Geographic Information Systems . in Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

MacQuoid-Mason D.J. (1978) *The Law of Privacy in South Africa.* Juta & Company Ltd. Kenwyn.

Madsen W. (1994) *Protecting Indigenous Peoples' Privacy from "Eyes in the Sky".* in Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

Marx G.T. (1994) *Some Information-Age Techno-Fallacies and Some Principles for Protecting Privacy.* in Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

McCullagh D. & Robinschon N. (1997) *No Privacy on the Web.* in Time, Time Warner Publishing, June 2, pg. 48-49.

Neethling, J., Potgieter, J.M. & Visser, P.J. (1996) *Neethling's Law of Personality.* Butterworth, Durban.

Neethling, J., Potgieter, J.M. & Scott, T.J. (1995) *Case Book on the Law of Delict.* Juta & Co. Kenwyn.

Neethling, J., Potgieter, J.M. & Visser, P.J. (1996) *Law of Delict.* 2nd Edition, Butterworth, Durban.

Onsrud, H.J., Johnson J.P., and Lopez X.R. (1994) *Protecting Personal Privacy in Using Geographic Information Systems.* in Photogrammetric Engineering & Remote Sensing Vol. 60, No 9. September. p. 1038-1095.

Peterson B.A. (1994) *Issues Concerning Access To Electronic Records.* in Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

Raab C.D. (1994) *European Perspectives on Protection of Privacy.* in Proceedings of the Conference on Law and Information Policy for Spatial Databases Tempe, AZ, October 29-31.

Rhind, D. (1992) *Data Access, Charging and Copyright and their Implications for Geographical Information Systems.* In International Journal of GIS. Vol. 6, No 1. January-February. p.13-30.

Wacks, R. (ed) (1993) *Privacy.* Volume II Privacy and the Law. Dartmouth Publishing Company Limited, Aldershot.

Wacks, R. (1980) *The Protection of Privacy.* Sweet & Maxwell, London.

Warren, S.D & Brandeis, L.D. (1890) *The Right to Privacy.* Harvard Law Review, 4, pp. 193-220.

Westin, A.F. (1967) *Privacy and Freedom.* In Wacks, R. (ed) (1993) *Privacy.* Volume II Privacy and the Law. Dartmouth Publishing Company Limited, Aldershot.

Interviews

Erasmus, A., Cape Town, 5/4/97.

Fagan, Dr A., Department of Private Law, University of Cape Town, 23/7/98.

Internet Sources

Ref 1 Commonwealth Consolidated Acts, Australia. *Privacy Act 1988 sect 14: Information Privacy Principles.* http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html. Date accessed: 31/7/98

Ref 2 Commonwealth of Australia, Attorney-General's Department. September 1996. *Privacy Protection in the Private Sector.* Discussion Paper. http://www.agps.gov.au/customer/agd/clrc/privacy.htm. Date accessed: 14/6/98

Ref 3 CORDIS RTD-NEWS. Record Control Number : 6162. 1996-05-21: *Commissioner Bangemann calls for agreement on core principles in development of Information Society.* http://www.cordis.lu/cordis-cgi/srchidabd.html. Date accessed: 27/4/98

Ref 4 Electronic Frontier Foundation. Dec 9 1997. *Policy on Public Interest Principles for Online Filtration, Ratings and Labelling Systems.* Draft Version 1.1b. http://www.eff.org/policies/filtration_policy.html. Date accessed: 14/6/98

Ref 5 Electronic Privacy Information Center (EPIC) – *Homepage.* http://www.epic.org. Date accessed: 10/6/98.

Ref 6 Electronic Privacy Information Center. April 7, 1996. *International Privacy Standards.* http://www.epic.org/privacy/intl/default.html. Date accessed: 10/6/98

Ref 7 EPIC Report 94-1*: Privacy Guidelines for the National Information Infrastructure – A Review of the Proposed Principles of the Privacy Working Group.* http://www.epic.org/privacy/internet/epic_nii_privacy.html Date accessed: 11/6/98

Ref 8 European Union. 23 November 1995. *EU directive 94 ECO 291 CODEC 92.* Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31. http://www2.echo.lu/legal/en/dataprot/directiv/ directiv.html. Date accessed: 12/5/98

Ref 9 Federal Trade Commission of the United States – *Homepage.* http://www.ftc.gov. Date accessed: 12/6/98

Ref 10 Federal Trade Commission. December 1996. *Public Workshop on Consumer Privacy on the Global Information Infrastructure* – Staff Report. http://www.ftc.gov/bcp/privacy/wkshp96/pw960604.pdf. Date accessed: 26/7/98

Ref 11 Federal Trade Commission. December 1997. *Individual Reference Services: A Report to Congress.* http://www.ftc.gov/bcp/privacy/ wkshp97/irsdoc2.htm. Date accessed: 16/6/98

Ref 12 Federal Trade Commission. June 1998. *: Privacy Online: A Report to Congress.* http://www.ftc.gov/reports/privacy3/priv-23a.pdf. Date accessed: 12/6/98

Ref 13 Federal Trade Commission. March 26, 1998. *Prepared Statement of the Federal Trade Commission on "Internet Privacy" before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary United States House of Representatives.* http://www.ftc.gov/os/9803/ privacy.htm. Date accessed: 12/6/98

Ref 14 Independent Newspapers 1998. *Data privacy law threatens to upset EU's relations with US.* http://www2.inc.co.za/archives/1998/9803/ 10/pri.html. Date accessed: 14/6/98

Ref 15 Individual Reference Services Group. December 15, 1997. *Industry Principles – Commentary (Final).* http://www.ftc.gov/bcp/privacy/ wrkshp97/irsdoc1.htm. Date accessed: 15/6/98

Ref 16 Individual Reference Services Group. December 15, 1997. *Individual Reference Services Industry Principles.* http://www.ftc.gov/bcp/privacy/wkshp97/irsgappd.pdf. Date accessed: 16/6/98

Ref 17 Industry Canada. *Privacy and the Canadian Information Highway* - Discussion Paper. http://info.ic.gc.ca/info-highway/ih.html. Date accessed: 14/6/98

Ref 18 Information Industry Association of US – *Homepage.* http://www.infoindustry.org Date accessed: 15/6/98

Ref 19 Information Industry Association. May 19, 1997. *Comments of the Information Industry Association in response to the Federal Trade Commission Request for Comments*: Data Base Study – Comment P974806 & Consumer Privacy 1997 – Comment P954807. http://www.infoindustry.org/ppgrc/doclib/grdoc003 and 008 and 009. Date accessed: 15/6/98

Ref 20 National Information Infrastructure. Privacy Working Group. Information Policy Committee. Information Infrastructure Task Force. June 6, 1995. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information.* http://www.iitf.nist.gov/documents/committee/ infopol/niiprivprin_final.html. Date accessed: 31/7/98

Ref 21 National Information Infrastructure Task Force. April 1997. *Options for Promoting Privacy on the National Information Infrastructure.* Draft for Public Comment. Information Policy Committee. http://www.iitf.nist.gov/ipc/privacy.htm. Date accessed: 12/7/98

Ref 22 OECD. 23 September 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/dsti/ sti/it/secur/prod/priv-en.htm. Date accessed: 27/4/98

Ref 23 OECD. 26 February 1998. *OECD Tackles Privacy on the Net.* http://www.oecd.org/dsti/sti/it/secur/act/privnote.htm: Date accessed: 14/6/98

Ref 24 Organization for Economic Co-operation and Development (OECD) – *Homepage.* http://www.oecd.org:. Date accessed: 26/7/98

Ref 25 Privacy International – *Homepage.* http://www.privacy.org. Date accessed: 18/6/98

Ref 26 Privacy International. 25 November 1991. *Interim Report of Privacy International Interim Report to Members 1990-1991.* http://www.privacy.org/pi/reports/interim_report_1991.html. Date accessed: 14/6/98

Ref 27 Privacy International. Date last modified: 15/4/1996. *Press Release*. http://www.privacy.org/pi/countries/australia/aus_priv_found_release.txt Date accessed: 14/6/98

Ref 28 W3C. 22 September 1997. *Platform for Privacy Preferences Project (P3P)*. http://www.w3.org/p3p/overview.html. Date accessed: 14/6/98

Ref 29 Weekly Mail & Guardian, 1996. *Put citizen rights first, says Nader* . by Mungo Soggot, June 28. http://www.gogga.ru.ac.za. Date accessed: 27/4/98

Table of Cases

Appendix 1 OECD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Source:

OECD. 23 September 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm. Date accessed: 27/4/98

APPENDIX 1

OECD

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Contents

PREFACE

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23rd September, 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

(23rd September, 1980)

THE COUNCIL,

Having regard to articles *1(c), 3(a)* and *5(b)* of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

- that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

  that automatic processing and transborder flows of personal data create new forms of relationships among

countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;

3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;

4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

- *a)* "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf:

  b) "personal data" means any information relating to an identified or identifiable individual (data subject);

  c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

- *a)* the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

  b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- *a)* as few as possible, and

  b) made known to the public.

5 . In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- *a)* with the consent of the data subject; or

  b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- *a)* to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data

relating to him;

b) to have communicated to him, data relating to him

1.
   - *within a reasonable time;*
   - *at a charge, if any, that is not excessive;*
   - *in a reasonable manner; and*
   - *in a form that is readily intelligible to him;*

- *c)* to be given reasons if a request made under subparagraphs*(a)* and *(b)* is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- *a)* adopt appropriate domestic legislation;

b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

e) ensure that there is no unfair discrimination against data subjects.

PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

1.
   - information exchange related to these Guidelines, and
   - mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Appendix 2 European Union

European Union – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Source:

European Union. 23 November 1995. *EU directive 94 ECO 291 CODEC 92.* Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31. http://www2.echo.lu/legal/en/dataprot/directiv/ directiv.html. Date accessed: 12/5/98

APPENDIX 2

European Union

This is an unofficial text. For the authoritative text of the Directive, reference should be made to the Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Other language versions: DE ES FR IT

Contents

webmaster@echo.lu

CHAPTER I GENERAL PROVISIONS

Article 1 Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2 Definitions

For the purposes of this Directive:

(a) 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b)'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d)'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h)'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3 Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by

Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II - GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I - PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II - CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III - SPECIAL CATEGORIES OF PROCESSING

Article 8 The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that' the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph I provided for in paragraphs 4 and 5 shall be notified to the Commission

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9 Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV - INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10 Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,
- the recipients or categories of recipients,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V - THE DATA SUBJECT'S RIGHT OF ACCESS TO

DATA

Article 12 Right of access

Member States shall guarantee every data right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred .to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI - EXEMPTIONS AND RESTRICTIONS

Article 13

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII - THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14 The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15 Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII - CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16 Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17 Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX - NOTIFICATION

Article 18 - Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19 - Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph I must be notified to the supervisory authority.

Article 20 Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21 - Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

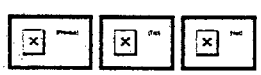
2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide provide of a legitimate interest.



CHAPTER III - JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22 Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in Question.

Article 23 Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the' provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV - TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25 Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26 Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate

legitimate interest, to the extent that the conditions laid down in law for consultation" are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V - CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI - SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28 Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political Institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29 -Working Party on the Protection of Individuals with regard to the Processing of

Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

.5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII - COMMUNITY IMPLEMENTING MEASURES

Article 31 - The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,
- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt

in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

Appendix 3 Information Industry Association

Information Industry Association Fair Information Practices Guidelines.

Source:

Information Industry Association. May 19, 1997. *Comments of the Information Industry Association in response to the Federal Trade Commission Request for Comments*: Data Base Study – Comment P974806 & Consumer Privacy 1997 – Comment P954807. http://www.infoindustry.org/ppgrc/doclib/ grdoc008 and 009. Date accessed: 15/6/98

APPENDIX 3

Information Industry Association

INFORMATION INDUSTRY ASSOCIATION

FAIR INFORMATION PRACTICES GUIDELINES
POLICY STATEMENT

In a Policy Statement on Privacy adopted by the IIA Board of Directors in 1990, IIA undertook to:

> *encourage companies in the information industry to explain clearly their policies and practices with respect to the collection, use and distribution of information, including steps taken to foster the security of information, and to keep information current and accurate. In this way, individuals may knowledgeably formulate realistic privacy expectations.*

In furtherance of the application of this Policy Statement to information regarding individuals, and as part of IIA's ongoing efforts to assist companies in their development of policies and practices, IIA has promulgated the following Fair Information Practices guidelines, which were adopted by IIA's Board of Directors February 26, 1994.

FAIR INFORMATION PRACTICES GUIDELINES

1. Companies are encouraged to:

a. **establish a policy on fair information practices regarding personally identifiable information they collect, use and distribute;**

b. **make this policy publicly available;**

c. **review the policy periodically and update it if needed; and**

d. **establish means and standards for monitoring compliance with the policy and establish accountability for it.**

Commentary: The business opportunity of maximizing information flow brings with it a responsibility to be sensitive to the use of information, particularly "personally identifiable information," which, for purposes of this statement, is defined as "information relating to an identified or identifiable individual." While this responsibility should be embodied in a written policy, this principle does not specify the policy's specific content. A variety of options should be considered with regard to making the policy public, ranging from dissemination in response to specific questions, to proactive publication and distribution. Alternative means for

monitoring and enforcing the policy include establishment of a corporate committee on fair information practices; annual business plan review of information practices; appointment of a high level manager within the company responsible for enforcing the policy; and conducting privacy impact assessments on new or existing products or services.

2. Companies are encouraged to:

take reasonable and appropriate steps to protect personally identifiable information against risks such as loss, and unauthorized access, use, modification, disclosure, or destruction. If such information is provided to third parties, companies are encouraged to require those third parties to have comparable protections.

Commentary: Information security is a key feature of responsible collection, use and distribution of personally identifiable information. While this principle does not amount to a guarantee, companies should recognize the customer service aspect of security measures.

3. Companies are encouraged to:

promulgate policies and practices that address the conditions associated with their receipt of personally identifiable information, including the following:

a. When such information is requested directly from the individual, the company is encouraged to disclose to him/her how it intends to use the information.

b. When a company obtains such information from other private sources, it should be used only for purposes consistent with the conditions under which it was obtained.

c. Collection, use and distribution of personally identifiable information should be in accordance with all applicable laws and regulations, including those pertaining to records collected by a government entity and made available to the public.

Commentary: The focus of paragraph (a) is to clearly inform the individual, from and about whom the information is obtained and of the purpose for which the information is being sought, which could include dissemination to third parties. This permits the individual to make an informed decision about whether to impose conditions on the company's use of the information. The principle does not address the timing of the notification.

Paragraph (c) recognizes that public record data obtained from government entities is generally accessible without restrictions on use. Where government entities have imposed restrictions, they must be complied with.

4. Companies are encouraged to:

take steps to attain and maintain the highest practicable level of information quality, consistent with industry practice and customer need.

Commentary: Information quality refers to the accuracy, completeness, and currentness of information. Personally identifiable information may be current or satisfy the other

criteria for one purpose but not another, so the required level of information quality depends upon the purpose for which the information will be used. This item recognizes that few practices are more destructive of customer and public confidence than maintaining inaccurate or outdated information.

4. Companies are encouraged to:

establish and implement an inquiry and inspection procedure, under which an individual can:

a. Learn if the company has personally identifiable information about him/her;

b. Have the information communicated within a reasonable time and under reasonable conditions;

c. Have the company correct or delete inaccurate or incomplete personally identifiable information, or, if appropriate, have the company identify the source of the information so that the individual can seek to have the inaccurate or incomplete information corrected or deleted;

d. Receive a prompt explanation if the company cannot fulfill an inquiry and inspection request, or if the company elects not to change or delete personally identifiable information which the individual has challenged as inaccurate or incomplete.

Commentary: While this principle encourages companies to establish appropriate policies to respond to concerns an individual may have about personally identifiable information a company collects, uses or distributes, it does not mandate particular procedures to address those concerns. Each company is best able to decide for itself what specific procedures to implement, taking into account factors such as the type(s) of information involved and the uses to which the information is put. For example, an inquiry and inspection procedure (and other aspects of the guidelines, such as policies on conditions associated with the receipt of information) may not be applicable to information obtained in the course of gathering news for publication.

With regard to paragraph (b): "reasonable conditions" include the format in which the information is communicated, whether written authorization is required, whether or not there is any charge for the information, etc. Again, each company is best situated to decide for itself what specific conditions are most appropriate, taking into account factors such as the subject's need for the information, the type of information involved, and the cost and difficulty of retrieving and providing the information.

With regard to paragraph (c): in most cases the company is in the position to change and correct the information, and should make reasonable efforts to make the correction or deletion in all appropriate company databases. However, in some cases, such as public record data on land ownership, the company cannot change the data even if it is incorrect. In such a case, the company could direct the subject of the information to the source of the information so that the subject may take appropriate corrective action. At its option, the company could undertake to inform the source directly of the asserted inaccuracy.

Comments on these guidelines should be forwarded to:

Daniel C. Duncan
Vice President Government Relations
Information Industry Association
1625 Massachusetts Avenue, N.W., Suite 700
Washington, DC 20036
(202) 986-0280; fax (202) 638-4403
dduncan@infoindustry.org

FAIR INFORMATION PRACTICES CHECKLIST

The following questions are designed to help your company develop or improve fair information practices or privacy/data protection policies. Circle your answers to each question to assess your company's position.

1. Does your company have a policy on fair information practices, privacy, or data protection regarding personally identifiable information (i.e., information relating to an identified or identifiable individual)? [If answer is NO, skip to question 5.]

   ○ YES ○ NO

2. Is the policy publicly available?

   ○ YES ○ NO

3. Is the policy reviewed periodically and updated if needed?

   ○ YES ○ NO

4. Does your company monitor compliance with the policy and establish accountability?

   ○ YES ○ NO

5. Does your company take steps to protect personally identifiable information against risks such as loss, or unauthorized access, use, modification, disclosure or destruction?

   ○ YES ○ NO

6. Does your company provide such information to third parties?

   ○ YES ○ NO

7. If so, does it require such third parties to take steps to protect the data?

   ○ YES ○ NO

8. Does your company request personally identifiable information directly from individuals? [If no, skip to question 10.]

   ○ YES ○ NO

9. Does your company inform the individual from whom it requests such information how it intends to use it?

C YES C NO

10. Does your company obtain personally identifiable information from other private sources (e.g., under license)? [If no, skip to question 12]

C YES C NO

11. If so, is the information used only for purposes consistent with the conditions under which it was obtained?

C YES C NO

12. Does your company obtain personally identifiable information from public records? [If no, skip to #14.]

C YES C NO

13. If so, does the company's use of the information comply with any restrictions imposed by government entities?

C YES C NO

14. Does your company take steps to maintain the highest practicable level of accuracy, completeness and currentness of personally identifiable information, considering the purpose for which the information will be used?

C YES C NO

15. Does your company have an inquiry and inspection procedure that individuals can initiate with respect to personally identifiable information relating to them?

C YES C NO

16. If so, under the procedure, can an individual:

    a. learn whether your company has personally identifiable information concerning him/her?

    C YES C NO

    b. have the information communicated within a reasonable time and under reasonable conditions?

    <INPUT name=`16b type=radio value=Yes> YES C NO

    c. receive a prompt explanation if the company (i) cannot fulfill the request, or (ii) elects not to change or delete personally identifiable information which the individual claims is inaccurate or incomplete?

    C YES C NO

17. If your company learns that its records contain inaccurate or incomplete personally identifiable information, does the company have a procedure for prompt correction or deletion of the information?

C YES C NO

18. If your company learns that its records contain personally identifiable information that is inaccurate or incomplete but that the company cannot effectively delete or correct (e.g., public record), does the company identify the source of the information to the individual upon request so that s/he can seek to have the information deleted or corrected?

○ YES ○ NO

RELATED DOCUMENTS

- IIA Comments in Response to "A Framework For Global Electronic Commerce" (Draft 9)
- Position Statement on Service Provider Liability for Copyright Infringement on Online Networks

Top of Page | Main Menu | GR Menu | PPGRC Document Library

Appendix 4 Individual Reference Services

Individual Reference Services Industry Principles

Source:

Individual Reference Services Group. December 15, 1997. *Individual Reference Services Industry Principles*. http://www.ftc.gov/bcp/privacy/wkshp97/irsgappd.pdf. Date accessed: 16/6/98

APPENDIX 4

Individual Reference Services

FINAL — DECEMBER 15, 1997

INDIVIDUAL REFERENCE SERVICES INDUSTRY PRINCIPLES

PREAMBLE:

The following principles were developed by members of the individual reference services industry to respond, as an industry, to heightened interest in the industry's practices. The principles represent good practices that the undersigned companies agree to support as part of their operating practices. While it may take up to a year for some principles to be implemented filly, other principles are already part of the operating practices of the undersigned companies.

SCOPE:

These principles apply to individual reference services, which are commercial services that directly or as suppliers to others provide information that assists users in identifying individuals, verifying identities and locating individuals for various purposes.

DEFINITIONS:

- *Public Record Information:* Information about or related to an individual which has been obtained originally from the records of a federal, state, or local governmental entity that are open for public inspection.

- *Publicly Available Information:* Information about an individual that is available to the general public from non-governmental sources such as telephone directories, classified ads, newspaper reports, publications, or other forms of information.

- *Non-Public Information:* Information about an individual that is of a private nature and neither available to the general public nor obtained from a public record.

- *Appropriate or Appropriately:* Describes actions or uses that are reasonable under the circumstances reflecting a balance between the interests of individual privacy and legitimate business, governmental, and personal uses of information, including prevention and detection of fraud.

PRINCIPLES:

I. *Education:* Individual reference services shall individually and through their industry groups make reasonable efforts to educate users and the public about privacy issues associated with their services, the types of services they offer, these principles, and the benefits of the responsible flow of information.

11, *Reputable Sources:* Individually identifiable information shall be acquired from only sources known as reputable in the government and private sectors.

A. Reasonable measures shall be employed to understand an information source's data collection practices and policies before accepting information from that source.

B. Individually identifiable information that is collected for marketing purposes shall not knowingly be purchased, sold or retained for creating or inclusion in individual reference services, unless it is PUBLIC RECORD INFORMATION or PUBLICLY AVAILABLE INFORMATION; its use is specifically permitted by law; or it is collected with notice to the individual that such information will be used for inclusion in individual reference service products.

III. *Accuracy:* Reasonable steps shall be taken to help assure the accuracy of the information in individual reference services. The goal of individual reference service products is to furnish customers with accurate reproductions of information.

A. When contacted by an individual concerning an alleged inaccuracy about that individual, the individual reference service, as APPROPRIATE, shall either correct any inaccuracy or inform the individual of the source of the information and, if reasonably available, where a request for correction may be directed.

B. The individual reference service's commitment to furnish users with reasonably accurate reproduction of information in PUBLIC RECORD INFORMATION systems does not permit alteration of the substantive content of PUBLIC RECORD INFORMATION products or services.

IV. *Public Record and Publicly Available Information:* PUBLIC RECORD INFORMATION and PUBLICLY AVAILABLE INFORMATION shall be usable without restriction unless legally prohibited.

V. *Distribution of Non-Public Information:* Except as provided in section IX, NON-PUBLIC INFORMATION will be distributed only according to the criteria set forth below. The nature of NON-PUBLIC INFORMATION being requested and the intended uses of such information shall determine the level of review of the subscriber. Companies who supply information covered by this section to individual reference services shall provide such information only to individual reference services that adopt or comply with these principles.

A. *Selective and Limited Distribution of Non-Public Information:* Individual reference services may distribute NON-PUBLIC INFORMATION without restriction of its contents only to qualified subscribers.

1. Qualified subscribers for the selective and limited distribution of NON-PUBLIC INFORMATION must satisfy the following conditions:

   a. The subscribers must state their APPROPRIATE uses for such information.

   b. The subscribers must agree to limit their use and redissemination of such information to such APPROPRIATE uses.

   c. The subscribers shall be reasonably identified and meet qualification requirements that establish them as APPROPRIATE users of the information and agree to terms and conditions consistent with these principles prior to accessing the information.

2. Each individual reference service shall take reasonable steps to protect against misuse of NON-PUBLIC INFORMATION distributed pursuant to this subsection which will include:

   a. Each individual reference service shall make available upon request an explanation of what uses of its information are APPROPRIATE and to which types of qualified subscribers such information is available.

   b. Individual reference services shall conduct a reasonable review of the subscriber and its intended uses of the information prior to making NON-PUBLIC INFORMATION available to the subscriber.

   c. Individual reference services shall maintain a record of the identity of subscribers, the types of uses, and the terms and conditions agreed to by the subscriber for three years after termination of each subscriber's relationship with the individual reference service.

   d. Reasonable measures shall be employed to help assure that qualified subscribers use NON-PUBLIC INFORMATION APPROPRIATELY.

   e. Individual reference services shall implement reasonable mechanisms to remedy subscriber abuses of the information.

B. *Commercial and Professional Distribution of Non-Public Information:* Individual reference services, when they limit the NON-PUBLIC INFORMATION content of their

products or services as set forth below, may distribute such products or services only to established professional and commercial users who use the information in the normal course and scope of their business or profession and the use is APPROPRIATE for such activities.

1. NON-PUBLIC INFORMATION products or services distributed pursuant to this subsection shall not include:

   a. Information that reflects credit history, financial history, medical records, mother's maiden name identified as such, or similar information;

   b. Certain information like social security number and birth information unless truncated in an APPROPRIATE and industry consistent manner.

2. Users shall agree to terms and conditions consistent with these principles prior to accessing the NON-PUBLIC INFORMATION, shall agree to use such information solely in the normal course and scope of their business or profession and that the use is APPROPRIATE for such activities and that they shall limit their use and redissemination of such information to such uses and in accordance with these principles.

3. Individual reference services shall take reasonable steps to protect against misuse of the NON-PUBLIC INFORMATION distributed pursuant to this subsection which will include:

   a. If not previously established, the individual reference service shall take reasonable steps to identify the user and to establish the user as an established professional or commercial entity.

   b. Reasonable measures shall be employed to help assure that commercial and professional customers use NON-PUBLIC INFORMATION APPROPRIATELY.

   c. Individual reference services shall implement reasonable mechanisms to remedy subscriber abuses of the information.

   d. Individual reference services shall maintain a record of the identity of subscribers and the terms and conditions agreed to by the subscriber for three years after termination of each subscriber's relationship with the individual reference service.

C. *General Distribution of Non-Public Information:* Individual reference services, when they limit the NON-PUBLIC INFORMATION content of their products or services as set forth in this subparagraph, may distribute such products or services to any person.

1. NON-PUBLIC INFORMATION distributed pursuant to this subparagraph shall not knowingly include information that reflects social security number, mother's maiden name identified as such, non-published telephone number, or non-published address information obtained from telephone companies, birth information, credit history, financial history, medical records, or similar information, nor will the service be retrievable by a social security number.

2. *The* individual reference service shall take reasonable steps to protect against the misuse of NON-PUBLIC INFORMATION.

VI. *Security*: Individual reference services shall maintain facilities and systems to protect information from unauthorized access and persons who may exceed their authorization. In addition to physical and electronic security, individual reference services shall reasonably implement:

A. Employee and contractor supervision-Employees and contractors shall be required to sign confidentiality agreements and be subject to supervision.

B. Reviews—System reviews shall be made at APPROPRIATE intervals to assure that employees are complying with policies.

VII. *Openness:* Each individual reference service shall have an information practices policy statement that describes what types of information it has, from what types of sources, how it is collected, the type of entities to whom it may be disclosed and the type of uses to which it is put, and shall make its policy statement available upon request. Consumers shall be notified about these practices in various ways such as:

1. Web sites;

2. Advertisements; or

3. Company or industry-initiated educational efforts.

VIII. *Choice:* Each individual reference service shall upon request inform individuals of the choices, if any, available to limit access or use of information about them in its data base, provided, however, that in the case of NON-PUBLIC INFORMATION distributed to the general public (section V.C of these principles), an individual reference service shall provide an opportunity for an individual to limit the general public's access or use of such NON-PUBLIC INFORMATION.

IX. Access: Upon request and reasonable terms, an individual reference service shall:

A. Inform an individual about the nature of PUBLIC RECORD and PUBLICLY AVAILABLE INFORMATION that it makes available in its products and services and the sources of such information;

B. Provide individuals with NON-PUBLIC INFORMATION contained in products and services that specifically identifies them and that are distributed as part of an individual reference service to users under section V. of these Principles unless the information was obtained on a limited use basis from a governmental agency or if its disclosure is limited by law or legally recognized privilege; and

c. Direct individuals to a consumer reporting agency regulated by the Fair Credit Reporting Act where such agency is the source of the information about the individual.

X. *Children:* Where an individual is identified in the product or service as being under the age of 18, no NON-PUBLIC INFORMATION about that individual shall be provided for other than selective and limited distribution purposes or for the purposes of locating missing children.

XI. *Assurance of Compliance:* The signers of these principles shall have completed within 15 months of the effective date of these principles. and on a periodic basis thereafter, at least once every year, an assurance review done by a reasonably qualified independent professional service. The independent professional service shall apply assurance criteria consistent with these principles and approved by the signers as a group. Individual referenceservices shall have a reasonable opportunity to respond to any concerns expressed in such assurance review. A summary reflecting both the [original] report and any subsequent actions taken or response made by the company shall be publicly available.

PLEDGE:

The undersigned companies pledge to introduce and follow the above industry principles at the earliest practicable opportunity or by December 31, 1998, whichever is sooner.

Acxiom Corporation
CDB Infotek, a ChoicePoint Company
DCS Information Systems
Database Technologies, Inc.
Equifax Credit Information Services, Inc.
Experian
First Data Solutions Inc.
Information America, Inc.
IRSC, Inc.
LEXIS-NEXIS
Metromail Corporation
National Fraud Center
Online Professional Electronic Network
Trans Union Corporation

Appendix 5 National Information Infrastructure

Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information

Source:

National Information Infrastructure. Privacy Working Group. Information Policy Committee. Information Infrastructure Task Force. June 6, 1995. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information.* http://www.iitf.nist.gov/documents/committee/infopol/niiprivprin_final.html. Date accessed: 31/7/98

APPENDIX 5

National Information Infrastructure

PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE:

PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION

Privacy Working Group

Information Policy Committee

Information Infrastructure Task Force

Final Version

June 6, 1995

PRINCIPLES AND COMMENTARY

I. General Principles for All NII Participants

1. Three fundamental principles should guide all NII participants. These three principles--information privacy, information integrity, and information quality--identify the fundamental requirements necessary for the proper use of personal information, and in turn the successful implementation of the NII. All NII participants should use appropriate means to ensure that these principles are satisfied.

I.A. Information Privacy Principle

Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.

2. The NII can flourish only if all participants respect information privacy. Information privacy is an individual's claim to control the terms under which personal information--information identifiable to an individual--is acquired, disclosed, and used. The level of privacy that must be respected is an individual's reasonable expectation, an expectation subjectively held by the individual and deemed objectively reasonable by society. Not all subjectively held expectations will be honored as reasonable. For example, an individual who posts an unencrypted personal message on a bulletin board for public postings cannot reasonably expect that personal message to be read only by the addressee.

3. What counts as a reasonable expectation of privacy under the Principles is not limited by what counts as a reasonable expectation of privacy under the Fourth Amendment of the United States Constitution. In many instances, society has deemed it reasonable to protect privacy at a level higher than that required by the Fourth Amendment. See, e.g., Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988); Right to Financial Privacy Act, 12 U.S.C. § 3401 (1988); Privacy Act, 5 U.S.C. § 552a (1988). The Information Privacy Principle fully supports such possibilities.

4. As explained in later principles and commentary, an individual's privacy can often be best respected when individuals and information users come to some mutually agreeable understanding of how personal information will be acquired, disclosed, and used. However, in certain cases--for example, if the individual lacks sufficient bargaining power--purely contractual arrangements between individuals and information users may fail to respect privacy adequately. In such instances, society should ensure privacy at some basic level in order to satisfy the Information Privacy Principle.

I.B. Information Integrity Principle

Personal information should not be improperly altered or destroyed.

5. NII participants should be able to rely on the integrity of the personal information the NII contains. Thus, personal information should be protected against improper alteration or destruction.

I.C. Information Quality Principle

Personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

6. Personal information should have sufficient quality to be relied upon. This means that personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

II. Principles for Users of Personal Information

II.A. Acquisition Principles

Information users should:

1. Assess the impact on privacy in deciding whether to acquire, disclose, or use personal information.

2. Acquire and keep only information reasonably expected to support current or planned activities.

7. The benefit of information lies in its use, but therein lies an often unconsidered cost: the threat to information privacy. A critical characteristic of privacy is that once it is lost, it can rarely be restored. Consider, for example, the extent to which the inappropriate release of sensitive medical information could ever be rectified by public apology.

8. Given this characteristic, privacy should not be addressed as a mere afterthought, once personal information has been acquired. Rather, information users should explicitly consider the impact on privacy in the very process of designing information systems and in deciding whether to acquire or use personal information in the first place. In assessing this impact, information users should gauge not just the effect their activities may have on the individuals about whom personal information is acquired, disclosed, and used; they should also consider other factors, such as public opinion and market forces, that may provide guidance on the appropriateness of any given activity.

9. After assessing the impact on information privacy, an information user may conclude that it is appropriate to acquire personal information in pursuit of a current or planned activity. A planned activity is one that is contemplated by the information user, with the intent to pursue such activity in the future. In all cases, the information user should acquire only that information reasonably expected to support those activities. Although information storage costs decrease continually, it is inappropriate to collect volumes of personal information simply because some of the information may, in the future, prove to be of some unanticipated value. Also, personal information that has served its purpose and is no longer reasonably expected to support any current or planned activities should not be kept.

10. The ability to acquire certain kinds of personal information does not mean that it is proper to do so. In certain cases, individuals have no choice whether to disclose personal information. For example, if the individual executes a transaction on the NII, personal information in the form of transactional data will typically be generated. In other cases, the choice may exist in theory only. Exercising certain choices may result in the denial of a benefit that individuals need to participate fully in society--for example, obtaining a license to drive an automobile. In such cases, society should establish some basic level of privacy protection in accordance with the Information Privacy Principle (I.A.).

II.B. Notice Principle

Information users who collect personal information directly from the individual should provide adequate, relevant information about:

1. Why they are collecting the information;

2. What the information is expected to be used for;

3. What steps will be taken to protect its confidentiality, integrity, and quality;

4. The consequences of providing or withholding information; and

5. Any rights of redress.

11. Personal information can be acquired in one of two ways: it can be collected directly from the individual or obtained from some secondary source. By necessity, the principles governing these two methods of acquiring personal information differ. While notice obligations can be placed on all those who collect information directly from the individual, they cannot be imposed uniformly on entities that have no such direct relationship. If all recipients of personal information were required to notify every individual about whom they receive data, the exchange of personal information would become prohibitively burdensome, and many of the benefits of the NII would be lost.

12. For those who collect personal information directly from the individual, the Notice Principle requires the individual to be given sufficient information to make an informed decision about his or her privacy. The importance of providing this notice cannot be overstated because the terms of the notice substantially determine the individual's understanding of how personal information will be used, an understanding that must be respected by all subsequent users of that information.

13. The Notice Principle specifically applies to personal information designated by law as a public record and to transactional data generated as a byproduct of a transaction. With respect to transactional data, this principle applies to all parties, including not only the party principally transacting with the individual in order to provide some product or service, but also to those transaction facilitators such as communication providers and electronic payment providers who help to consummate these transactions. For example, if an individual purchases flowers with a credit card through an on-line shopping mall accessed via modem, the Notice Principle applies to all parties who collect transactional data related to the purchase, not only to the florist, but also to the telephone and credit card companies. Transaction facilitators would ordinarily provide notice at the time they establish an account, or when billing the customer.

14. What counts as adequate, relevant information to satisfy the Notice Principle depends on the circumstances surrounding the collection of information. In some cases--especially where there is a continuing relationship between the individual and the information collector-- notice need not be given before each instance that personal information is collected. For example, an information or communication service provider should ordinarily give notice when the individual subscribes to a particular service and perhaps periodically thereafter, not each time the individual uses the service. In other cases, the ordinary and acknowledged use of personal information is so clearly contemplated by the individual that providing formal notice is not necessary. For example, if an individual's name and address is collected by a pharmaceutical company that takes the order over interactive television simply to deliver the right medicine to the right person at the right address, no elaborate notice need precede taking the individual's order. However, should the pharmaceutical company use the information in a manner not clearly contemplated by the individual--for example, to create and sell a list of people afflicted with high blood pressure to health insurance companies--then some form of notice should be provided.

15. While the Notice Principle indicates what might constitute the elements of adequate notice, it does not prescribe a particular form for that notice. Rather, the goal of the Principle is to ensure that the individual has sufficient information in an understandable form to make an informed decision. Thus the drafters of notices should be creative about informing in ways that will help all individuals, regardless of age, literacy, and education to achieve this goal.

16. Finally, although the Notice Principle requires information collectors to inform individuals what steps will be taken to protect personal information, they are not required to provide overly technical descriptions of such security measures. Indeed, such descriptions might be unwelcome or unhelpful to the individual. Furthermore, they may be counterproductive since widespread disclosure of the technical security measures might expose system vulnerabilities, in conflict with the Protection Principle (II.C.).

II.C. Protection Principle

Information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.

17. On the NII, personal information is maintained in a networked environment, an environment that poses tremendous risk of unauthorized access, disclosure, alteration, and destruction. Both insiders and outsiders may gain access to information they have no right to see or may make hard-to-detect changes in data that will then be relied upon in making critical decisions.

18. For example, our health care providers expect to become intensive participants in the NII. Through the NII, a hospital in a remote locale will be able to send x-rays for review by a radiologist at a teaching hospital in another part of the country. The potential benefits are obvious. Yet, such benefits will not be realized if individuals refuse to send such sensitive data because they fear that the NII cannot ensure that sensitive medical data will remain confidential and unaltered.

19. In deciding what controls are appropriate, information users should recognize that personal information should be protected in accordance with the individual's understanding and in a manner commensurate with the harm that might occur if it were improperly disclosed or altered.

20. In protecting personal information, information users should adopt a multi-faceted approach that includes both technical and managerial controls. As for technical controls, information users should, for example, consider encrypting personal information, including the contents of communications and information generated from transactions. In addition, they should consider computerized audit trails, which help detect improper access by both insiders and outsiders. As for management controls, one could strive, for example, to create an organizational culture in which individuals learn about fair information practices and adopt these practices as the norm. Also, organizations could establish policies to forbid information acquired for one activity from being used for another unrelated activity.

II.D. Fairness Principle

Information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.

21. An individual's understanding encompasses the individual's objectively reasonable contemplation and scope of consent when the information was collected. As explained earlier, an individual's understanding depends principally on the notice provided by the information collector pursuant to the Notice Principle (II.B.) and obtained by the individual pursuant to the Awareness Principle (III.A.). Without a Fairness Principle, information use may know no boundaries and thus go beyond the individual's understanding.

22. If an information user seeks to use personal information in an incompatible manner, the user must first notify the individual and obtain his or her explicit or implicit consent. The nature of the incompatible use will determine whether such consent should be explicit or implicit. In some cases, the consequences to an individual may be so significant that the prospective data user should proceed only after the individual has specifically opted into the use by explicitly agreeing. In other cases, a notice offering the individual the ability to opt out of the use within a certain specified time may be adequate. Inherent in this principle is the requirement that whenever personal information is transferred from information user to user, the individual's understanding of how that personal information will be used must also be conveyed. Because all information users must abide by the Fairness principle, both information transferor and transferee bear a responsibility to ensure that the individual's understanding is transferred along with the information.

23. In deciding whether a particular use of information is "incompatible" with an individual's understanding, information users should evaluate whether the uses are permitted explicitly in the notice or are otherwise consistent with the notice. Any use of information beyond these conditions is incompatible with the individual's understanding. What is incompatible under this Principle is not limited to what has been interpreted as incompatible under the Privacy Act. See 5 U.S.C. § 552a.

24. The Fairness Principle cannot be applied uniformly in every setting. An incompatible use is not necessarily a harmful use; in fact, it may be extremely beneficial to the individual and society. There are some incompatible uses that will produce enormous benefits and have at most a trivial effect on the individual's information privacy interest. Research and statistical studies, in which information will not be used to affect the individual, are examples. Obtaining the consent of the individual to permit new statistical uses of existing data adds cost and administrative complexity to the process and risks impairing the research project. In other cases, personal information may be used for a significant public need recognized by society in a highly formal, open way (typically in legislation) that would be thwarted by giving the individual a chance to limit its use. One example would be the use of personal information in a law enforcement investigation for which the suspect's consent would be unlikely and even asking for such consent would be counterproductive to the investigation. Another example would be an incompatible use of personal information, made by the investigatory press, that is specifically protected and sanctioned by the First Amendment.

II.E. Education Principle

Information users should educate themselves and the public about how information privacy can be maintained.

25. The Education Principle represents a significant addition to the traditional principles of fair information practice. There are many uses of the NII for which individuals cannot rely completely on governmental or other organizational controls to protect their privacy. Although individuals often rely on such legal and institutional controls to protect their privacy, many people will engage in activities outside of these controls, especially as they engage in the informal exchange of information on the NII. Thus, individuals must be aware of the hazards of providing personal information, and must make judgments about whether providing personal information is to their benefit.

26. The full effect of the NII on the use of personal information is not readily apparent, and individuals may not recognize how their lives may be affected by networked information. Because it is important that individuals and information users appreciate how the NII affects information privacy, all information users should participate in education about the handling and use of personal information. Traditionally, governments and schools have educated the public on matters of social rights and responsibilities, and they must continue to play a lead role. However, as major builders of the NII, the private sector has as crucial a role to play. Such education, which would help individuals minimize the risks to their privacy, could involve privacy telephone hotlines, Internet privacy "help" sites, and comprehensive marketing and publicity campaigns.

III. Principles for Individuals Who Provide Personal Information

III.A. Awareness Principle

Individuals should obtain adequate, relevant information about:

1. Why the information is being collected;

2. What the information is expected to be used for;

3. What steps will be taken to protect its confidentiality, integrity, and quality;

4. The consequences of providing or withholding information; and

5. Any rights of redress.

27. Increasingly, individuals are being asked to surrender personal information about themselves. Sometimes the inquiry is straight-forward; for example, a bank will ask for personal information prior to processing a loan request. In this case, one use for the information is clear--to process the loan application. There may, however, be other uses that are not so obvious, such as using some of that information for a credit card solicitation. Indeed, individuals regularly disclose personal information without being fully aware of the many ways in which that information may ultimately be used. For example, an individual may not realize that paying for medical services with a credit card creates transactional data that could reveal the individual's state of health.

28. The Awareness Principle recognizes that although information collectors have a responsibility to inform individuals why they want personal information, individuals also have a responsibility to understand the consequences of providing personal information to others. This is especially true in an interactive realm such as the NII, in which individuals can actively shape the terms of their participation. For example, when individuals have real choices about whether and to what degree personal information should be disclosed, they should take an active role in deciding whether to disclose personal information in the first place, and under what terms.

29. Of course, if individuals are to be held responsible for making these choices, they must be given enough information to make intelligent choices. This is how the Awareness Principle works in conjunction with the Notice Principle (II.B.) and more broadly with the Education Principle (II.E) to enable individuals to take responsibility over how personal information is disclosed and used.

III.B. Empowerment Principles

Individuals should be able to safeguard their own privacy by having:

1. A means to obtain their personal information;

2. A means to correct their personal information that lacks sufficient quality to ensure fairness in its use;

3. The opportunity to use appropriate technical controls, such as encryption, to protect the confidentiality and integrity of communications and transactions; and

4. The opportunity to remain anonymous when appropriate.

30. Individuals should have a means to obtain from information users a copy of their personal information and to correct information about them that lacks sufficient quality to ensure fairness in its use. The extent to which such means are provided depends on various factors, including the seriousness of the consequences to the individual of using the personal information and any First Amendment rights held by the information user.

31. Further, if the terms of the information collection are unsatisfactory, the individual should consider various self-initiated measures to safeguard privacy. For example, to safeguard the confidentiality or integrity of a communication, the individual should have the opportunity to use appropriate tools such as encryption. Also, to avoid leaving a data trail of transactional records, individuals should have the opportunity to remain anonymous, when appropriate. For example, anonymity would be appropriate when an individual browses a public electronic library or when an individual engages in anonymous political speech protected by the Constitution. See McIntyre v. Ohio Elections Commission, 131 L. Ed. 2d 426 (1995). In an ideal world, offering undecipherable encryption or absolute anonymity would serve to protect privacy with no negative effect. Unfortunately, in the real world, some will abuse these technologies and, in the process, harm others. It is beyond the scope of the Principles how encryption or anonymity can be offered to individuals for legitimate uses while minimizing their misuse. These issues must, however, be addressed if the NII is to achieve its full potential.

III.C. Redress Principle

Individuals should, as appropriate, have a means of redress if harmed by an improper disclosure or use of personal information.

32. Redress is required only when an individual is harmed. Designed for general applicability, the Redress Principle does not answer in any particular case whether harm has occurred at all or whether enough harm has occurred to warrant a specific form of redress. Those questions must be answered in the sectoral implementation of the Principles.

33. An improper use specifically includes a decision based on personal information of inadequate quality--information that is not accurate, timely, complete, or relevant for the purpose for which it is provided and used. The Redress Principle does not, however, set the level of culpability on the part of the information user necessary to warrant a specific form of redress.

34. When redress is appropriate, the Principles envision various forms including, but not limited to, informal complaint resolution, mediation, arbitration, civil litigation, regulatory enforcement, and criminal prosecution, in various private, local, state, and federal forums with the goal of providing relief in the most cost-effective manner possible.

PWG/IPC: june6.nii

/1/ See Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Annex to Recommendations of the Council of 23rd September 1980. .

Appendix 6 Information Privacy Principles

Australian Privacy Act 1988 sect 14: Information Privacy Principles

Source:

Commonwealth Consolidated Acts, Australia. *Privacy Act 1988 sect 14: Information Privacy Principles.* http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html. Date accessed: 31/7/98

APPENDIX 6

Information Privacy Principles

PRIVACY ACT 1988 - SECT 14

Information Privacy Principles

The Information Privacy Principles are as follows:

INFORMATION PRIVACY PRINCIPLES

Principle 1

Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

(a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

(b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law--the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4

Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5

Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the record-keeper has possession or control of any records that contain personal information; and

(b) if the record-keeper has possession or control of a record that contains such information:

(i) the nature of that information;

(ii) the main purposes for which that information is used; and

(iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

(a) the nature of the records of personal information kept by or on behalf of the record-keeper;

(b) the purpose for which each type of record is kept;

(c) the classes of individuals about whom records are kept;

(d) the period for which each type of record is kept;

(e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

(f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6

Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7

Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8

Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9

Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10

Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the individual concerned has consented to use of the information for that other purpose;

(b) the record-keeper believes on reasonable grounds that use of the

information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

(d) the disclosure is required or authorised by or under law; or

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.