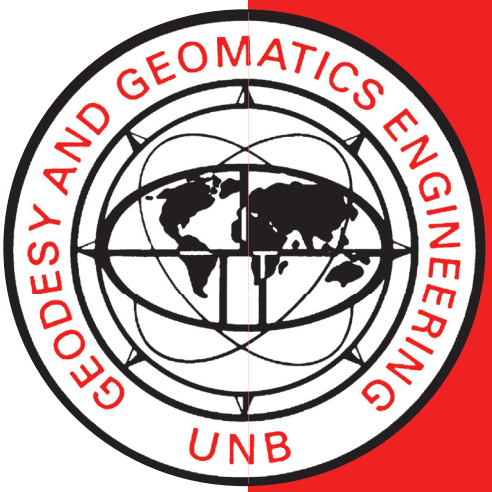
ACCESS AND PRIVACY OF DISTRIBUTED LAND RELATED INFORMATION

R. I. ANDERSON

August 1992



TECHNICAL REPORT
NO. 161

PREFACE

In order to make our extensive series of technical reports more readily available, we have scanned the old master copies and produced electronic versions in Portable Document Format. The quality of the images varies depending on the quality of the originals. The images have not been converted to searchable text.

ACCESS AND PRIVACY OF DISTRIBUTED LAND RELATED INFORMATION

Ralph I. Anderson

Department of Surveying Engineering
University of New Brunswick
P.O. Box 4400
Fredericton, N.B.
Canada
E3B 5A3

August 1992

PREFACE

This technical report is a reproduction of a thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering in the Department of Surveying Engineering, July 1992. The research was supervised by Dr. John McLaughlin, and funding was provided by the South Australian Department of Lands.

As with any copyrighted material, permission to reprint or quote extensively from this report must be received from the author. The citation to this work should appear as follows:

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.

Abstract

As information technology evolves and the perception of the value of information changes, the legal solutions designed to provide checks and balances for qualities such as information access and privacy are struggling to stay abreast of social and technological developments. The ease with which vast arrays of information may be accessed in a distributed computing environment was not foreseen by the authors of much of the legislation and policy in place today.

The issues of information access and privacy can not be discussed in isolation. Satellite factors such as information ownership, distribution, pricing, liability and security all have an impact and must be taken into account. Consideration of these issues must play a part in policy formulation.

After studying existing and proposed legislation, principles and policies, components have been isolated which should find a place in any policy that deals with access and privacy for land related information in a distributed environment. The guidelines formulated are generic in nature and do not address jurisdiction dependant idiosyncrasies.

In addition to the policy components, a development strategy is proposed. The main thrusts of the strategy are that the policy should attempt to be: media independent; applicable to all sectors of society, especially when dealing with the issue of privacy; encouraging of a proactive approach to information dissemination; and, aware that privacy is a vital quality that must be considered in coincidence with all access decisions.

The combination of the components and the development strategy provides a framework that will prevent discontinuities and inconsistencies in the application of the policy. The suggestions made should prove useful in the development of access and privacy policies for land information in a distributed information environment that are appropriate, effective and applicable both now and in the future.

Table of Contents

Abstract ii
Table of Contents iii
List of Figures vii
Acknowledgements viii

1. Introduction 1
1.1. The Information Society 2
1.1.1. Information as a Commodity 3
1.2. Distributed Information Environment 6
1.3. The Importance of Access and Privacy 10

2. Access 12
2.1. Levels of Public Information 12
2.2. Levels of Availability 13
2.3. Reasons for Access 14
2.4. Access for Commercial Reasons 15
2.5. Freedom of Information Legislation 16
2.6. Equity 17
2.7. Access and Technology 17
2.8. The Need for Access 19

3. Privacy 22
3.1. Exemption from Disclosure 23
3.2. Misgivings about Technology 24
3.3. Data Matching and Sharing 25
3.4. Public Sector/Private Sector Anomalies 26
3.5. Reasonable Use of Information 27
3.6. Privacy Erosion 27
3.7. Existing Policies 28
3.8. Privacy and Land Related Information 29

4. Influencing Factors 32
4.1. Distribution 33
4.1.1. Distribution Mechanisms 34
4.1.2. Wholesaling and Retailing 35

4.1.3. Private Sector Efficiency 36
4.1.4. Selection Criteria 37
4.2. Pricing 38
4.2.1. Justification for Charging 40
4.2.2. Cost Recovery Options 40
4.2.3. Partial Cost Recovery Model 41
4.2.4. Discretionary Pricing 42
4.2.5. Balanced Pricing Policy 43
4.3. Ownership of Information 44
4.3.1. Intellectual Property Rights 44
4.3.1.1. Patents 45
4.3.1.2. Trade Secrets 45
4.3.1.3. Protection and Use of Information 45
4.3.2. Copyright 46
4.3.3. Custodianship 48
4.3.4. Summary 51
4.4. Liability 51
4.4.1. Duty of Care and Third Party Liability 53
4.4.2. Limiting Liability 53
4.4.3. Summary 55
4.5. Impact on Access and Privacy 56
4.5.1. Control of Information 58
4.5.1.1. Use of Copyright 59
4.5.1.2. Use of Freedom of Information Legislation 59
4.5.2. Commercialization and Competition 61

5. Security 63

5.1. Attributes of Security 65
5.1.1. Confidentiality 65
5.1.2. Integrity 65
5.1.3. Availability 66
5.1.4. Utility and Authenticity 66
5.1.5. Priority of Attributes 67
5.2. Technical Network Security 67
5.2.1. Special Nature of Distributed Environments 68
5.2.2. Identity 69
5.2.3. Authentication 69

5.2.4. Authorization 70
5.2.5. Secure Communications 71
5.2.6. Auditing 71
5.3. Levels of Security 72
5.4. Information Classification for Access Control 74
5.4.1. Information Vulnerability 77
5.4.2. Classification of Information 78
5.4.3. Determining Correct Classification 81
5.4.4. Protecting and Managing Information 82
5.5. Balanced Use of Security 85
5.5.1. The Cost of Security 85
5.5.2. Policy and Technology 86

6. Access and Privacy Policy Development 88
6.1. Generic Information 88
6.1.1. Existing Legislation 89
6.1.1.1. Access 89
6.1.1.2. Privacy 91
6.1.1.3. Complementary Nature of Privacy and Access 93
6.1.2. Proposed Legislation 93
6.1.3. Existing Policies 95
6.1.3.1. Circular A-130 95
6.1.3.2. Canadian Policies 96
6.1.4. Principles 97
6.1.4.1. ACUS 98
6.1.4.2. GODORT 99
6.1.4.3. OECD 100
6.1.5. Summary 103
6.2. Land Related Information 103
6.2.1. Existing Legislation 104
6.2.2. Existing Policies 106
6.2.2.1. United States 106
6.2.2.2. Canada 108
6.2.2.3. Australia 110

6.3. Land Information Access and Privacy Policy Development 112
6.3.1. Commitment to Information Access 113
6.3.2. Access Mechanisms 114
6.3.3. Equity 115
6.3.4. Privacy 116
6.3.5. Security 117
6.3.6. Information Ownership 117
6.3.7. Pricing 118
6.3.8. Role of the Public and Private Sectors 118
6.3.9. Liability 119
6.3.10. Conditions of Use 120
6.3.11. Summary 120

7. Conclusion 124

References 127

Legislation Cited 140

Appendix I OECD Guidelines 141

Appendix II Australian Privacy Act Information Privacy Principles 144

Appendix III ACUS Recommendation 88-10 151

List of Figures

Figure 1.	Distributed Information Environment	8
Figure 2.	Dimension of the Private/Public Choice	34
Figure 3.	Issues Related to Ownership	58
Figure 4.	Concentric Levels of Protection	74
Figure 5.	Access Control Matrix	183
Figure 6.	An Access Rule	84
Figure 7.	Penetration Work Factor Versus Cost	86
Figure 8.	Components of an Information Access and Privacy Policy	121

Acknowledgements

I wish to thank:

- the South Australian Department of Lands, and Surveyor General Mr. J.R. Porter in particular, for their financial support and commitment to the pursuit of progressive ideas;
- my supervisor, Dr. John McLaughlin;
- fellow Land Studies Group students, especially Sue Nichols and Ray A. Moore, for providing an atmosphere conducive to discussion;
- my parents, for their quiet encouragement and faith;
- Carolyn and Kate, who joined me on this adventure and provided all the support needed.

1. Introduction

Increasing computing power and sophisticated telecommunications technology are making the development of distributed information systems a reality. The use of such a distributed environment provides a new and powerful means of gathering, processing and disseminating a vast array of information products. There are, however, some facets to this environment which are not adequately dealt with by current policies in many jurisdictions. Some of the institutional issues which appear to be floundering in the wake of rapid advances in information technology relate to the ownership of information, the role of the private and public sectors in the distribution of information, the rights of access to information, and information privacy. It is the goal of this thesis to analyse existing and proposed legislation, policies and principles relating to information, and from this analysis to suggest components and strategies that should be used in the development of access and privacy policies suitable for land related information available through a distributed information environment.

The issues at hand are generic to all information and indeed are often discussed at length in relation to personal information. The purpose of this study, however, is to illuminate the problem from the perspective of land related information. In this thesis, land information and land related information will both be given the very broad definition of,

> that encompassing information about natural resources, the environment, land ownership, land use, transport, communications, mapping, demographic and socioeconomic factors where such information can be related to a geographic position. This applies to landmass, aquatic, atmospheric or subsurface area [ALIC, 1990b].

The term land related information refers to a very broad genre of information, which due to its extensive base has an appreciable impact on a wide variety of decision making activities. Information falling within this category could well be used to form the basis for the bulk of all action. The consumers of such information are diverse.

The diversity, and possible disparity, in the needs and rights of all parties involved in the use of land related information can only hope to be satisfied by the balanced deployment of information technology and policies which specifically recognize and address information issues. The combination of computerized data and communication networks may provide a solution to some of the perceived inadequacies and inequities relating to information use within the community, but their union may also result in a number of

problems which could threaten some of the basic rights assumed in any free and democratic society. Consideration of these potential problems should ideally result in the development of policies which clearly enunciate the balance to be struck between such issues as access and privacy, while at the same time allowing flexible use of technology and development of new information products to satisfy the needs of users.

1.1. The Information Society

> The functioning of society depends upon information and the efficient communication of it among society's members. In the broadest sense, the social, cultural, political and economic institutions in any society are defined in the terms of the characteristics of the shared information within these institutions. In the narrower economic sense, it has been recognized generally that the most important resource determining the economic efficiency of any economy, industry, production process or household is information and its effective communication [Melody, 1981].

The environment in which this thesis is set is known as the information society. An information society can be broadly defined as one in which the majority of people are employed in occupations concerned with the flow of information, rather than in agriculture or industry. MacLean [1984] offers the following comprehensive definition.

> ...[An] information society is taken to be any society which exhibits the following characteristics which are points on a continuum, instances of an evolutionary mode:
>
> 1. the generation, processing, storage and distribution of information employs the largest portion of the workforce;
>
> 2. these activities are recognized as a potential source of wealth rather than simply a cost of doing business;
>
> 3. the production of systematized, formal knowledge is the main agent of social change;
>
> 4. intelligent systems provide significant control mechanisms in all major social and economic sectors;
>
> 5. these mechanisms are on the point of passing from the augmentation of human intellectual process to their automation.

An information society is only the most recent form of the evolution of human society. Toffler [1980] refers to the information society as the 'third wave'. The first wave was the agricultural society, in which land and labour became the most important components. The second wave was the industrial society, in which the elements of capital, energy and skill

became the most important. In the third wave, the information society, information and knowledge are key resources. The information revolution allows for the mental powers of humans to be magnified, just as the industrial revolution brought about an increase in the physical capabilities of humans [Jones, 1984]. The increased reliance on mental endeavour within the information society has resulted in information and knowledge supplanting labour and energy as central variables of the economy [Lyon, 1988].

The catalyst for the information society is the development and convergence of computer and telecommunication technology [Lyon, 1988]. This combination, unlike any other before it, uses as raw material , or input, the inexhaustible and infinite resource of data and information to produce a final product [Hamrin, 1981]. Information, however, can not provide shelter, food, or any of the basic physical necessities of life. An information society is not economically independent; it relies on being able to trade its product for agricultural and industrial sector products.

The ability to derive economic wealth from the trade of information is dependant on at least two factors. These factors are somewhat generic to the sale of all goods and are present, in only marginally altered form, when the products of agricultural and industrial societies are traded.

- "An open and available global telecommunications system is essential to survival" [Branscomb, 1986]. This is the means of getting the product to the market. No wealth can be generated if the product can not be distributed to users.
- The ability to protect ownership rights in information. There must be some means of preventing those who have not paid from using the information.

The coming of the information age brings changes of an economic, social, cultural and political nature. The handling of these changes requires some degree of skill. It is unlikely that the transition to an information society will be completely painless or without a certain amount of confusion. Fundamental changes are required in the way that information itself is viewed. It must be recognized as a resource, a commodity of economic value. Inevitably conflict will arise over the best and proper use of this resource.

1.1.1. Information as a Commodity

Information is widely recognized as one of the most critical and essential of corporate resources [Schweitzer, 1990]. Information has a pivotal role to play in meeting the needs of a large number of markets. As a consequence, the market characteristics of information

are not static, but change to suit the needs of the users it seeks to satisfy. Information markets can be broadly classified into two categories [Melody, 1981]:

- Highest market value is achieved by maximum dispersion of the information. Information falling into this category is usually that which is designed for mass consumption by the public. Examples include weather forecasts and entertainment television. It is worth noting that in an agricultural or industrial society, information often attains its highest value when freely distributed, as this may lead to productivity increases in the basic economic activity (e.g., information about crop strains or industrial processes is distributed to promote increased productivity which in turn is beneficial to the society as a whole).
- Highest market value is achieved by restricting the availability of information to users who value it for its scarcity and seek an advantage by having exclusive knowledge of specific information. This form of information is generally that which is used to gain an advantage over market competitors. In an information society it is often necessary to view information in this light.

The value of information is highly subjective and is determined by how useful it is perceived to be by a particular user in a given set of circumstances. An information product's usefulness is ultimately judged according to the characteristics desired or needed by the user. One means of increasing the objective value of information is to increase its quality. Quality is a difficult term to define, but is described by some of the characteristics listed below:

1. *Currency.* The data must be accessible in an up to date form within a time frame that meets the needs of the user.
2. *Precision.* The data must provide measurement information to the standard that is required. Thus underground facilities, for example, must be recorded to a precision which they can be dug up expeditiously.
3. *Accuracy.* There must be little or no error in the information extracted from the data. Where possible error exists, the degree of probability of its correctness should be available. There should be guarantees , as in the registration of title, in which anyone who loses because of errors in the registration process can receive compensation.
4. *Verifiability.* Different users should be able to get the same answer to the same question.
5. *Clarity.* The information must be free from ambiguity.
6. *Quantifiability.* Where appropriate, numerical information should be obtainable.

7. *Accessibility*. It should be possible to extract information quickly and easily.
8. *Freedom from bias*. There should be no alteration or modification to the raw data in order to influence those who receive them.
9. *Comprehensiveness*. The data should be complete in spatial cover and content. Financial constraints may, however, prevent this and priority areas must therefore be completed first.
10. *Appropriateness*. The information derivable from the data should relate to the potential users' requirements [Dale and McLaughlin, 1988].

In an information society, information takes on some of the characteristics of traditional commodities such as material, labour and energy. As with any resource of economic value there are certain questions which can be asked of it, such as:

- who has it?
- who wants it?
- how can you get it?
- what are the terms of trade? [McLaughlin, 1991]

The above characteristics are common to all resources. Information, however, has some additional characteristics which are very special. The uniqueness of these characteristics can in part be attributed to the facts that information is not a non-renewable resource [Hamrin, 1981] and that it is not physical in nature. Information can be distinguished from traditional material goods due to the following properties:

1. Not consumable – goods are consumed by being used, but information remains no matter how much it is used;
2. Non-transferrable – in the transfer of goods from A to B, they are physically moved, but in the transfer of information, it remains with A;
3. Indivisible – materials, such as electricity and water, are divided for use, but information can only be used as a 'set';
4. Accumulative – goods accumulate when they are not used, but information cannot be consumed or transferred, so it is accumulated by being used repeatedly [Dale and McLaughlin, 1988].

In conclusion, "information is a resource that offers great opportunity to the business that manages, develops and applies it to making better decisions" [Schweitzer, 1990]. It is the ability of information to reduce uncertainty and lead to better decisions that establishes it

as a commodity of value. It should be noted, however, that it is not the amount of information that has the greatest impact on the decision making process and the resultant outcome, but the quality of the information and its relevance to the situation at hand.

1.2. Distributed Information Environment

If the first tenet upon which this thesis is based is that information is an item of significant economic worth and can be treated as a tradeable commodity, then the second is that one of the means of realizing maximum value of land related information is by allowing it to be disseminated and used in a distributed information environment. For the purposes of this text, a distributed information environment is one in which "a computer network connects any number of independent computers, often at geographically remote locations, so that they can communicate with each other and share programs, data and hardware" [Gould, 1989].

The fact that every major computer vendor now supports some form of distributed network computing [Milliken, 1990] indicates that the distributed computing trend, started in the 1980s, will continue to be a dominant theme in the 1990s [McBride and Brown, 1991]. Gould [1989] contends that computer networks may be considered the nervous system of the information society. They enable communication between autonomous nodes and facilitate the use of all resources found within the commonwealth of the network.

Depending on how it is implemented, a distributed information system can allow a high degree of local autonomy, permitting individuality, creativity and flexibility at each node, or it can enforce a highly structured schema which results in an almost centralized appearance to the user [Elmasri and Navathe, 1989]. Whatever the appearance to the user, however, the distribution of the database is the critical factor which differentiates such a system from previous concepts. The use of a distributed database, defined as "a collection of data that belongs logically to the same system but is physically spread over the sites of a computer network" [Elmasri and Navathe, 1989], endeavours to create an environment in which the flow of information between all users is improved. This improvement can lead to, and be facilitated by, decreasing the high costs of repeated duplication of data, increasing the integrity of the common store of data, and establishing the ability to integrate data from different sources in a coherent manner.

The implementation and operation of a distributed database is influenced by three main variables:

- Degree of homogeneity – refers to the differences in the systems found at each node in the network. If all nodes use the same software and the same data schema, the environment is deemed to be homogeneous. If differences are present between the nodes, the environment is said to be heterogeneous [Elmasri and Navathe, 1989].
- Degree of local autonomy – a distributed database system with no local autonomy appears as a single centralized system to the user. Administration of such a system by the database administrator takes place at a single central node. This central administrator enforces the use of a single conceptual schema for the whole system. Whereas a distributed database system with little local autonomy is logically centralized but physically decentralized, a system which is both physically and logically decentralized gives rise to a high degree of local autonomy [Elmasri and Navathe, 1989; Webster, 1988].
- Degree of distribution transparency – this is the key to realizing the full benefits of a distributed system [Milliken, 1990]. "The degree of distribution transparency describes to what extent data decentralization is hidden from the user" [Lee and McLaughlin, 1991]. If the system has a high degree of distribution transparency the user is not required to specify where the data resides when a request is made. Distributed database management systems which hide the details of data distribution make it easier for users, but require more complex software to enable this to occur.

One example of the way in which organizations may be interconnected as a result of the use of networks is depicted by figure 1. This model can be used to portray a number of scenarios relating to who owns the databases, who will distribute the data, at what stage value-adding can be carried out, etc.

In the model depicted, the client is able to gain information by one of two means. Firstly, the client may interact directly with the required database, or databases, to obtain the data sought. This route requires the client to have some knowledge of the technical aspects of using the network, although ideally these should not be a severe impediment. If desired, the client could then do any value-adding using his or her own resources (hardware, software and data). Alternatively, the client may approach an intermediary agency to obtain a particular piece of information. If the intermediary is a private sector organization, it is likely that the selection of that company by the client will be based on a particular value-adding process which the company is capable of providing.

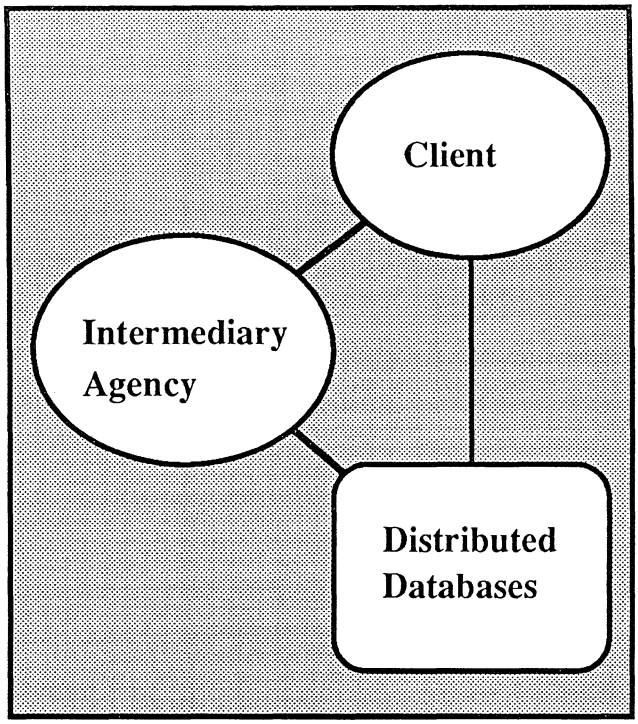


Fig. 1. Distributed Information Environment (after Anderson and Moore, [1991])

In an ideal market economy, the intermediary agency would not be a public sector organization. In such an economy all information deemed to be 'public' in nature would be directly available to individual citizens, or private sector intermediaries, via the network. There would be no need for a client to wish to gain access to data through the government. In reality, this is unlikely to occur. There are at least two reasons for this:

- The public sector may be involved in providing some value-added information products. This may be due to a need in the market not being met by the private sector, or the public sector dabbling in retailing in order to recoup some or all of its costs.
- There may be some information collected and stored by government which although dispensed upon request is not readily available for direct access by the public.

A distributed database may contain information contributed from a variety of sources within both the public and private sectors. Some databases may be controlled by the public sector, but contain information wholly, or in part, generated by the private sector. Other databases may be wholly created and maintained by private sector companies. What is important with regard to distributed databases is not who 'owns' them, but that access be

facilitated via the network. This creates an environment permitting maximum utilization of data resources within the community.

Connecting the various nodes in the system is the communication network. This is the hardware and software which enables electronic communication of data and information between nodes. The use of this form of communication enhances the ability to transfer large quantities of data between users, and can lead to significant increases in efficiency and effectiveness if whole communities are connected and make use of the service.

The growing use of distributed systems, which is driven by the rising performance/cost ratio of technology and increasing global competition, reflects both technical and organizational forces [Summers, 1989]. A combination of these forces has led to the appreciation of the value to be gained from sharing data and applications. Reduced costs and improved services can be simultaneously achieved by enabling a user to instantaneously access and update information in a database at any time from any location [McBride and Brown, 1991].

The gains to be made from integrating information from a variety of sources result from both the avoidance of costs and the realization of previously unattainable benefits. The distributed computing environment places resources, in a logical sense, where they are most needed. Each component in the system is able to assist in the performance of required tasks, resulting in greater reliability and responsiveness. Data and information are integral elements in the system. In an ideal system, information moves about in a controlled and user-transparent manner.

As the model depicted in figure 1 shows, in a distributed information environment data may be stored at physically remote locations, but all users have the ability (to varying degrees) to gather and enter data into the database, and to copy or use data from the distributed store of data. It is an egalitarian system in which all users have the potential to play a part in all aspects of the database life-cycle (creation, maintenance, use, etc.). "But no matter how it is technically defined, what a network ultimately networks are human beings with minds" [Gould, 1989]. A distributed information environment will ultimately give rise to a range of moral and policy questions for those who use, abuse or are in some way affected by the environment. On the positive side, participation in the distributed environment can lead to greatly enhanced social cooperation and interaction.

1.3. The Importance of Access and Privacy

"There are major transformations concerning legal protection of property rights in information based upon the increased value of information in an information society" [Branscomb, 1986]. These transformations affect both access to information and privacy of information. On the one hand, access to databases is necessary if the potential benefit contained in the collection of information is to be realized. On the other hand, individuals have a right to expect that their privacy will not be infringed as a result of misuse of information. A balance must be struck between allowing disclosure and use of information, ostensibly for the overall good of the community, and protection of personal information privacy.

One of the potential threats to the development of a truly successful information-based society is a lack of equitable access to information. Current technological developments appear to be moving toward a point where, thanks to the availability of inexpensive hardware and software, universal information access is technically feasible in the more developed countries [Fitzsimmons, 1987]. The development of policies which ensure equitable access to information must be encouraged to match the remarkable advances in information technology. Technical capability is of no value if policies are not in place to foster an environment in which organizations are willing (indeed desirous) to become part of a network and permit access and use of their data resources.

The creation of a truly equitable information society is also threatened if individuals are not afforded some degree of control over information which relates directly to them. These rights may range from control over the collection of information in the first place, to how information is to be used after collection has taken place. The acceptance of ownership rights in information is a logical corollary when information is regarded as a valuable commodity.

Chapters two and three of this thesis will discuss the issues of access and privacy in greater depth. These two issues have been debated at length in relation to personal information. At first glance, land information may appear to be somewhat less contentious, however, the very broad definition of land information which has been adopted and advances in information technology provide ample opportunity to discover the socially fractious (if not divisive) components of these matters.

Chapter four will address some of the institutional issues that have a direct bearing on access and privacy. While it is not the intention of this thesis to become embroiled in the debate over the distribution and pricing of information, it is felt that these subjects certainly

warrant some discussion. Likewise, the issue of ownership of information needs to be explored to promote an understanding of the underlying issues that must be taken into account when formulating policy which addresses access and privacy. The liability of providing and producing information will also be addressed.

Chapter five will look at security, particularly as it applies to a distributed computing environment. Although primarily a technical matter, this issue will also be addressed from a policy perspective. Emphasis will be placed on the value of classifying information by using objective guidelines to determine when, to whom and under what circumstances information should be made available. It is hoped that such a system may lend itself to the resolution of conflict between access and privacy.

Chapter six will examine examples of existing legislation, proposed legislation, policies and principles which impact on access to and privacy of information. Strong features of these examples will be identified, and areas in which weaknesses are detected will be addressed. The goal is to compose guidelines dealing with access and privacy of electronically stored land related information.

The guidelines composed must be cognizant of the variable manner in which members of the community view information in certain circumstances. Information may have: a public value, which translates into a right to access to records; a private value, reflected in a concern about disclosure of personal and proprietary information; and a commercial value [Epstein, 1990]. A framework must be suggested which provides not only a safety net against abuse, but furthers proactive development of policies which encourage and enhance the use of information in a distributed environment.

2. Access

> Access to personal and geographic information depends on law, economics and culture as well as technology. Law and the legal process determine the extent of disclosure or confidentiality of data and information [Epstein, 1990].

"Information has been described as the currency of democracy" [OECD, 1983]. The principle of access to information is rooted in the theory that widespread use of information is necessary for the development of an informed public and an accountable government and is of great benefit to society as a whole. Access to government-held information enables the public to review the same records the government uses in forming its decisions.

With the advent of new technologies which enable assimilation and analysis of vast volumes of information, and the changing perception of the value of information as a commodity, existing positions on access to information are increasingly less germane to the realities of the situation. Access to information is the most pressing issue in a distributed information environment and deserves appropriate analysis.

2.1. Levels of Public Information

When the topic of access to information is raised it is necessary to differentiate between public information and other types of information held by government. Public information is data and information that is gathered, received, processed, managed, or otherwise used by a government agency in the normal course of its mandated activities [Epstein, 1992]. Some of this public information is held by government for the express purpose of making it available for use by the public. Records contained within public registries exemplify this type of information. This information is a matter of public record. Other information held by government, although available upon request, is not gathered primarily for use by the public. This form of information may be of interest to individuals and special interest groups, but is not intentionally collected for purposes related to public notice. Its principal purpose is to aid in the internal functioning of government. Yet other information gathered and stored by government is not intended to be available for scrutiny by the general public under any circumstances. Its use may even be restricted within government. Information contained within such records may be necessary or helpful in administering the mandate of the agency, however, certain elements may be unsuitable for use by the public due to their personal, proprietary or sensitive nature.

2.2. Levels of Availability

Epstein [1990] posits that a distinction should be made between the concept of access to information and that of disclosure or non-disclosure of information. Disclosure of government-held information is a matter of public policy which deals with what information may and may not be revealed to the public. Access to information, on the other hand, is not truly a matter of public policy, but a means of implementing the policy of disclosure or non-disclosure. Public access to information refers to any method by which the public may examine, reproduce, or otherwise obtain information from a government entity [Hernon and McClure, 1984].

Having made the distinction between the right to information and the means by which that right can be implemented, Perritt [1990] describes three levels at which information release may occur: access, disclosure and dissemination. It should be noted that Perritt uses the term disclosure in a different sense than Epstein.

- Access to information occurs when citizens are provided with information, to which they are legally entitled, upon their request [Berman, 1989]. "Access is the lowest level and most passive form of information release. The agency must release information upon request but is not affirmatively required to do so" [Perritt, 1990]. Information which is subject to access requirements only is often stored and presented in a manner which is suitable for use within the responsible organization, but not for easy retrieval or use by the general public.
- Disclosure occurs when information is made available to the public in one or more places. It is an intermediate level of release that requires some degree of affirmative effort to make the information more easily obtainable. The effort required may amount to the establishment and maintenance of public viewing rooms equipped with the hardware and software necessary to permit retrieval of information from databases.
- Dissemination refers to activities in which "government provides [the] public with information without [the] public asking for it" [Perritt, 1990]. The aim is to make information "widely available to [the] public at places where it it used" [Perritt, 1990]. In a distributed environment, dissemination may require the establishment of dial-up links to permit remote access to the database or databases by modem. Ease of retrieval and other user friendly features are characteristics of a system in which dissemination is the target environment.

From a policy and administration perspective, the distinction between access and dissemination is important in defining boundaries which are useful in settling disputes such as the difference between providing access to existing records or creation of new information, and charging nominal fees or the full cost of information production. In an electronic distributed environment, however, the distinction between access and dissemination is becoming increasingly artificial [Kahin, 1991]. Providing for the online availability of a database is deemed to be a dissemination activity, especially if the data is intelligently indexed and ordered and a user-friendly interface is established to help automate handling. At the same time, the initiative for accessing the database and obtaining the information must come from the individual, not the government agency controlling the data, so the activity may be deemed to be that of access.

2.3. Reasons for Access

Traditionally, access to information legislation has been based on the principle that information collected by government at public expense should be available to the public if for no other reason than to allow the public to make an assessment of government actions [Leia, 1989]. The tenor of federal freedom of information legislation in both Canada and the U.S. is directed towards government agencies and their holdings of data. The purpose of freedom of information legislation is "...to enhance the accountability of the government in its administration of public policy by allowing the citizen to have the necessary information upon which to form a rational judgement as to the adequacy of that administration" [Bell, 1988]. In this sense, access to government-held data is required for the public to carry out some form of audit on its government.

Access to government and privately held data stores may also be required by individuals or organizations to check that information stored about themselves is correct. Personal or financial damage resulting from the use of incorrect information stored in a database could be extreme. In such circumstances access to information is required to verify the integrity of the information itself.

With the coming of the information age and the realization of the varied uses and values of information, these traditional reasons for access form only part of the argument for gaining entry to data stores. More and more, members of the community desire to use information in a pro-active manner. Newly developed skills and the availability of the necessary equipment have led to the realization by portions of the public that they have the ability to effectively use and analyse information from public databases for themselves [Berman, 1989]. Such people are now interested in gaining access to information in order

to determine answers to problems, rather than merely viewing information as an end in itself. This trend has even evolved to the point where government-held records may be desired by those seeking commercial gain from a resource that is under-utilized.

This third reason for desiring access to information results from:

- a desire to increase the efficiency with which certain tasks in the community are undertaken by the intelligent use of information to decrease costs and/or increase benefits;
- an increased awareness of the commercial value of certain information.

2.4. Access for Commercial Reasons

Government carries out three distinct activities which have a significant influence in the marketplace:

- regulation of private enterprises;
- direct participation in the marketplace;
- planning of future growth and development [Soloway, 1980].

The information collected or generated by government to facilitate these functions may be of great commercial value to the private sector. If accessible, such information could prove commercially beneficial by decreasing the 'unknown element' present in all business decisions. A decrease in the perceived level of risk in a venture, brought about by the availability of relevant information, may lead to increased levels of investment.

The commercial value of computerized government databases and information systems passes unrecognized by most freedom of information legislation [Roitman, 1988], although this situation is slowly changing [Dando, 1991]. Recognition of commercial value requires an associated acknowledgement of rights of an economic and legal nature. For information these rights are still in their infancy and have not yet been universally formalized.

In the U.S., limitations on access to information may be based on the purpose of the request. In some states, requests made to gain information for commercial purposes may be refused [Roitman, 1988; Dando, 1991]. Instances of such limitations to access are diminishing and are now found in very few states [Archer, 1988]. One interesting statistic from the U.S. comes not from companies seeking information for commercial purposes, but rather from companies seeking information for unfair commercial advantage. It has been estimated that 80% of requests for information have been made by businesses seeking to learn the secrets of their competitors [Trottier, 1988].

Private sector vendors of information are not subject to the same degree of regulation as government agencies. A number of Canadian provinces have enacted legislation governing the collection and use of information about individuals which is intended to be sold to third parties [Leia, 1989]. Essentially, however, the marketplace governs access to such privately held databases.

2.5. Freedom of Information Legislation

Freedom of information legislation (also known as right to information legislation or open records laws) is the vehicle through which a party may request the government to disclose certain records. Such legislation relates specifically to public information holdings and has no bearing on privately owned databases. To date "freedom of information has been overwhelmingly a public sector debate" [OECD, 1983]. Although made almost ten years ago, this statement still holds true today to a large extent.

There are three basic aims underpinning most freedom of information legislation:

- protect the rights of individuals to access information about themselves held by government and the right to correct that information if it is false or misleading;
- enable wider access to information gathered at public expense;
- improve the quality of decision making [Bayne, 1984].

When conflict between disclosure and confidentiality arises, freedom of information legislation generally requires access to be granted to all records except those defined by very specific exemptions. These exemptions relate to information, the release of which could unfairly compromise security, justice, commercial activity, personal privacy, etc. While certain exemptions are listed in freedom of information legislation, other legislation may also prevent or restrict the disclosure of records which fall within the jurisdiction of that legislation. Such legislation may override the legal authority of freedom of information legislation [Province of New Brunswick, 1990].

One of the intentions of freedom of information legislation is to make non-confidential and non-sensitive government records available to any member of the public upon request. The right to information upon request is equivalent to Perritt's [1990] definition of a right to access (see section 2.2.). According to the Department of Justice, Canada [1987] a right to access is the extent to which freedom of information legislation may operate. Such legislation is intended to serve in a request-responsive manner rather than in a disclosure or dissemination sense. Freedom of information legislation is intended to be used only as a last resort after all other avenues have been exhausted.

2.6. Equity

The concept of equity encompasses several principles which are summarized in the following definition. "Individuals, groups and organizations within our society should be afforded access to necessary activities and services under rational and consistent rules and procedures" [Office of Technology Assessment, 1982]. Arbitrary imposition of disadvantage on some groups, and unearned enrichment of others, and the capricious alteration of options, rights, responsibilities and benefits are clearly inequitable.

Cost is one means by which equity can be reduced. Freedom of information legislation attempts to redress this problem by requiring requested information to be supplied at what are termed reasonable costs. These costs are generally a nominal fee to cover the expense of amassing and copying the information. So called 'purse string' regulation of access to information is discouraged.

Electronic dissemination technologies might also have an effect on the equity of information accessibility. The advantages of operating in a distributed environment with digital information are obvious. Logically then, those unable to take advantage of the benefits are disadvantaged and inequity exists. While the potential for great advantages and great equity exists, if access to the technology is prevented or inhibited, perhaps even by a lack of technical knowledge or confidence required to participate in the environment, then inequity is created [Office of Technology Assessment, 1988; Doctor, 1991].

2.7. Access and Technology

Most freedom of information legislation explicitly recognizes its applicability to computerized information. For instance, most legislation makes no distinction between records held on paper or in electronic format. In the U.S. very few states base exemptions to the disclosure of information on reasons connected with the computerized nature of the information. While much of the legislation refers to computerized information, most of it was enacted prior to the information technology revolution [Roitman, 1988]. Legislation is often difficult to apply to technical advances and trends, the occurrence of which were never envisaged.

Three areas in which difficulty and confusion are being encountered as a result of the introduction of information technology are:

- medium of choice;
- creation of new records;

- reasonable search effort [Office of Technology Assessment, 1988].

When freedom of information legislation is invoked, the medium on which information is made accessible may be a source of contention. Should government agencies supply information in the format requested, or is it only necessary to make the information accessible in the least expensive form, or the form most compatible with the agency's current delivery modes? Those public sector organizations adopting a more commercial approach to the dissemination of the information in their keeping, are likely to be more willing to supply information in a wide range of formats, especially those formats that are most sought after by the market.

Technological advances can also make it difficult to determine how far a government agency should go in satisfying an information request. Freedom of information legislation requires that government agencies search for and provide information if it is not exempt from disclosure. This requirement does not, however, obligate agencies to answer questions, generate explanatory material, compile statistical data, or provide information that is not contained in existing records. In short, there is no requirement to create new records to meet a request. If an organization is operating in an automated environment the question must be asked, what is a 'search', and what is the 'creation of a new record'.

Requests for data under freedom of information legislation need only be met if they can be satisfied by a reasonable search effort. The use of computers and electronically stored databases facilitates faster and more complex searches for information, thereby broadening the definition of a reasonable search. The point at which a search develops into the creation of a new record is becoming difficult to distinguish.

One means of maintaining a distinction between searching and record creation in an electronic environment is by assessing whether the search activity is functionally analogous to that which would occur if the process were done manually. For example, the retrieval of data from a database does not constitute the creation of new records, even though some form of programming may be required to select certain specified fields. Such a search is functionally analogous to a manual search, even though an equivalent manual search may have required a great deal of effort or expenditure of resources.

The distinction between 'records in being' and 'information in the abstract' is obscured by information technology. Information technology effectively detaches information from its tangible form. Data stored electronically is incomprehensible and only becomes a useful body of information upon retrieval. The retrieval process requires some form of

manipulation or analysis of the digitally stored data. Consequently, the database should be thought of as an information 'pool' rather than a collection of discrete records.

With advancing technology providing an ever expanding range of means by which to gain access to information, it is becoming increasingly difficult to maintain the balance between privacy and access. Information technology is developing at such a rate that the line between public and confidential information is becoming blurred. Much can currently be done to 'de-personalize' information and conversely, there is much specific personal data that can be extracted by combining separate records which individually are not confidential. The main issue then, when dealing with searching or creating new records, becomes one of creating new relationships between the data and whether such actions can be objectively justified, especially in the event of liability incurred as the result of the use of that information. In the electronic environment, determination as to whether access is permissible needs to focus on the substance, or information content, of databases, rather than the operations required to extract or interpret data.

2.8. The Need for Access

The differing speeds with which technology, social values and policies are evolving must be handled carefully. It is necessary to react not by keeping technological developments in check, but rather by trying to adapt and take advantage of the opportunities presented by technology. It is important, however, that policies relating to disclosure of information be driven not by advances in information technology, but by the desire to most effectively meet the needs and values of society.

Difficulties in providing or maintaining an adequate level of access to information are decreasingly the fault of deficiencies at the technical level. Technical issues are being actively pursued and can effectively be discounted as factors likely to prevent the realization of the desired environment [Glenn, 1989]. The great challenge lies in understanding and addressing institutional issues and how they impact on such matters as the human communication process and in identifying with greater clarity and objectivity the uses of information [Budd, 1987]. Such factors as an overwhelming volume of data, or a lack of clarity, accuracy and simplicity in the information may thwart the use of information more effectively than any technical inadequacy [Hondius, 1987].

When dealing with government-held records, there are two tenets which must be resolutely protected:

- equity of access – all people must have an equal opportunity to access the information;
- access to personal information must be protected if a breach of privacy is likely to result.

These two points seem to figure in the results of freedom of information litigation in the U.S. Regarding access to land information the following four points are recurrent:

- a disposition in favour of access;
- an eagerness to place new technology in the service of access;
- an insistence on no more than reasonable charges for requested information;
- a sensitivity to concerns of privacy when the law is shown to be relevant to those concerns [Behrens, 1985].

Looking beyond the traditional role of the government in data collection, and the reasons for disclosure or non-disclosure, it would seem that there has been an evolution in the requirements of data users. This evolution is evidenced in new reasons for wanting information, and new expectations of government in supplying information. Both of these can be said to have sprung from the realization of the value of information. This value may be commercial in nature. Alternatively, the value may be intangible in that use of the information results in outcomes, for the good of the public or individuals, to which it is difficult to attach a definite dollar value.

The following statement both expresses a position about the changing nature of government in providing access, and poses some questions as to the complete development of the concept.

> ...the public is now beginning to look at government as an information generator on a wider scale – even as a generator of information that has commercial value. The question arises, as yet not fully answered, as to whether government should be a more active provider of information. Is it enough for government to provide information on request, or should government be engaged in a broader function of gathering and disseminating information as an essential service? [Province of New Brunswick, 1990]

The needs of an information hungry society can only be sated by proactively meeting its desires. If effective and controlled access is to be provided, policies must address themselves to information content, rather than the physical manifestation of data. Any policy that adequately addresses information itself, will necessarily provide guidance on

such matters as access equity, the commodity nature of information, the role of the public and private sectors in the distribution of information, and the threat to personal privacy brought about by the inappropriate use of information and information technology.

3. Privacy

Privacy is important in a society where people are to be free to go about their own business unhindered. Yet the concept is difficult to protect, mainly because it is hard to define. A simple, generally stated, definition of privacy is "the right to be left alone." A more comprehensive definition is "the claim of individuals, groups and institutions to determine for themselves when, how and to what extent information about them is communicated to others" [Westin, 1967]. From these two definitions it can be seen that privacy is a relative value; it varies depending on time, circumstance, and culture.

The concept of privacy is held dear by many societies (as reflected in their legislation) and this high regard "reflect[s] a concern about disclosures of personal and proprietary information that are unreasonably detrimental or favourable to individuals or organizations" [Epstein, 1990]. While the concept of privacy is generally deemed to be of great importance, the courts have yet to develop clear and consistent principles of information privacy [Office of Technology Assessment, 1986].

Information privacy, by which the flow of information about an individual is controlled by that individual, is of immediate interest to this thesis. There are, however, several other perspectives from which privacy may be viewed:

- territorial privacy – this involves recognition of some spatial location and an individual's rights within and over that physical area;
- personal privacy – personal autonomy which promotes bodily integrity and the sanctity of human dignity [Flaherty, 1991].

Prosser [1960] analysed four distinct torts that represent four types of privacy invasion:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

These categories, however, all depend on physical invasion or require publicity [Office of Technology Assessment, 1986]. Although the second category, that of public disclosure of private facts, would appear to come close to addressing information privacy,

the courts have interpreted that none of these four categories protects the individual from the acquisition, storage and transfer of information [D'Elia and Lunin, 1991].

Privacy has been described as "one of the most difficult and perplexing issues of our time" [Dansby, 1991]. When dealing strictly with land information we are often reticent to perceive any threat to privacy. What is of concern is that attributes, some of which may be considered confidential or sensitive by certain parties, may be attached to the land. An obvious corollary to this is that once attributes, even if they are harmless when viewed in isolation, have been entered into a database, they may be combined with specific elements of other selected databases to create new information that infringes on the rights of privacy of a target group [Gould, 1989].

There are generally three conditions that determine when disclosure of facts violates privacy:

1. the facts are not public knowledge and not easily available to public inspection;
2. there is public disclosure or publication;
3. the information made public is such that a person of ordinary sensibilities would object to its publication [Snapper, 1989].

3.1. Exemption from Disclosure

In an effort to provide protection of privacy, freedom of information legislation recognizes certain types of information that should be exempt from disclosure. The classes of exempt information include: (see for example [N.B. Right to Information Act, 1978; U.S. Freedom of Information Act, 1974; Canadian Access to Information Act, 1985])

- foreign policy/national defense matters;
- criminal investigations records;
- attorney opinions;
- proprietary and private business information;
- information exempted by other legislation;
- medical records;
- personal information;
- negotiation related information.

If a database contains information, the disclosure of which would constitute an invasion of privacy, this information may be exempted from disclosure. It is the intention of freedom of information legislation that class exemptions be very specific and narrowly interpreted [Archer, 1988]. As a result, it is often the case that certain data contained in a general data set is excluded from disclosure due to its confidentiality, while the remainder of the data is made available. This process is known as severance.

3.2. Misgivings about Technology

Computers, although commonplace now, are a relatively new technology. It is only since the early 1980s that their use has become widespread. This newness creates caution in the minds of many. These people are not necessarily 'technophobes' but merely wary and perhaps have a healthy awareness of the things that can go wrong [Globe and Mail, 1990].

Misgivings about technology may indeed be well founded, judging by the ease with which information may be obtained, analysed and disseminated. The main fear is that personal information will be accessed, resulting in an invasion of privacy. While much of the information available today has always been available, the introduction of technology has made the accessibility and use of these records much easier. Previously, paper records provided a form of latent protection from invasion of privacy due to their scattered and poorly documented nature. It was difficult to retrieve information, to be certain that all available information had been retrieved, to analyse the information, etc. Their use would have resulted in an unacceptable consumption of resources and the task would have been practically impossible [Epstein, 1990].

Absolute control over information becomes more difficult as computer networks create new ways of obtaining information about individuals. It may be possible to create a composite profile of an individual by linking information from selected databases. The information in each of these databases may be classified as public information, may be innocent enough by itself, and may even have been offered voluntarily. The compilation of the data, however, may reveal more about the individual than was intended, or may create information for which consent was never obtained. The information content of certain databases, after selective combination and analysis, may be greater than the sum of the parts [Nickel, 1989]. In this manner, the privacy of individuals may be "systematically violated in ways of which they are not even aware" [Gould, 1989].

The proliferation of electronically stored databases poses a fundamental challenge to privacy because of the awesome ability of computers to collect, store and disseminate data.

Computers are capable of a great many tasks at high speed and at low cost. It is precisely these qualities which concern people. A computer is capable of gathering, combining and distributing information very rapidly, but it is not capable of being discrete. It is unable to make judgements about the sensitivity of the information it is creating, as it is unaware of the context in which the information will be used [Fox, 1976].

There are various other misgivings about technology and its use, such as the misuse of sensitive data by unauthorized personnel, etc. Chapter five will discuss these and other issues in greater detail in the context of security. At this stage it is sufficient to note that in one particular study, 77% of the respondents believed that "as long as information is stored on computers, we can never be sure of our guarantee to privacy" [Linden, 1988]. This fear has not decreased in the intervening years. A poll carried out in 1990 found that four out of five American consumers "expressed general fear about threats to personal privacy" [Kozub, 1991].

3.3. Data Matching and Sharing

A certain amount of apprehension exists on the part of the general public about the ability of information to be aggregated and disaggregated [Epstein,1990]. The power of new technology enables large amounts of data to be assembled and analysed with great ease, enabling functions that were once virtually impossible, to be carried out at the press of a button. Two such activities which have great potential for mismanagement, and subsequent invasion of privacy, are data sharing and data matching [Macartney, 1988].

Data sharing is one method used to attempt to optimize the utilization of a distributed data set. It employs a common pool of data across multiple organizations [Province of British Columbia, 1991]. Through data sharing, organizational efficiency can be increased by reducing the amount of storage required for a system to be operational and effective. Data integrity may also be increased as a result of having only a single data source. Data sharing can also be used in a more aggressive manner to detect such undesirable activities as fraud [Macartney, 1988].

Data matching involves the linking of two or more separate databases by the use of a common identifier, usually a personal identifier, usually for the express purpose of making decisions about the individuals to whom the data pertains. On the surface, computer matching appears to offer great benefits in detecting fraud, waste and abuse of government welfare and social service programmes and the like [Hendricks, 1988]. The potential for erroneous matches, however, has been proved to be great [Cavoukian, 1988] and strict controls must be maintained to ensure that individuals are not falsely accused.

"The prospect of compiling inaccurate, obsolete or incomplete information on individuals through data matching is one of the most serious risks posed by record linkages" [Privacy Commissioner of Canada, 1989]. If individuals are not to be penalized as a result of erroneous data matches, 'due process' must be a principle to which investigators strictly adhere. Due process requires that all information produced as a result of a matching process be verified and that the individual, or individuals, in question be given the opportunity to state their case before any action is taken. Obviously, claims of invasion of privacy will be levelled by those being accused. For this reason, it is necessary to consider, prior to the instigation of a data matching programme, whether the benefits to be gained outweigh the invasion of privacy that will result [Privacy Commissioner of Canada, 1989].

3.4. Public Sector/Private Sector Anomalies

The existence and use of government-held data has been emphasized to date. The extent of privately held information should, however, not be underestimated. "The collection and dissemination of private information by the commercial sector is diverse and amorphous" [Dansby, 1991]. The direct mailing marketing industry in the U.S., for example, maintains databases which detail the interests of 90 million households [Mitchell, 1990], and the three largest American credit information companies each maintain records on 150 million individuals [Flaherty, 1991]. While there is a great deal of apprehension about the aggregation of information, the public generally accepts, although in a grudging manner, the existence of such privately held databases (credit information, consumer spending habits, etc.) in exchange for the perceived advantages that are received from them [Epstein, 1990].

It has been stated that information is a commodity. In the public sector the realization of the value of this strategic corporate asset is only just beginning to become apparent to many data custodians. In the private sector, the commodity qualities of information have long been exploited. Lists that contain the names and addresses of people who subscribe to various papers, journals and magazines are bought and sold. In Canada there are currently more than 900 direct mailing lists being rented or exchanged on a regular basis [Mitchell, 1990]. With so much activity in the information marketplace, clearly there needs to be some regulation or control to prevent the rights of individuals form being disregarded.

3.5. Reasonable Use of Information

There is no doubt that privacy is a valuable and essential attribute within society. As with anything, however, if given too much weight, anomalies will result that are just as great as those that would occur if privacy is given insufficient heed [Burkert, 1987]. In societies in which the information industry accounts for the largest portion of the workforce it is not possible, nor may it be desirable, to forbid the collection and computerization of all information about individuals [Wacks, 1989]. It is important to develop means of accommodating legitimate needs for gathering information while respecting the rights of individuals to privacy [Moor, 1989].

An example of legitimate needs can be found in the development of public policy. Policy based on accurate information is likely to be better that one that is developed in the absence of such information. This example is merely a subset of the truism that information is needed for good decision making. An obstacle may be encountered, however, when an attempt is made to use information for purposes other than that for which it was intended, even if that purpose is for the good of the community [Moor, 1989].

It is at this point that computers, far from being the villain so often associated with privacy violations, may be found to be of great benefit. Using standard information technology tools it is a simple matter to form insensitive data from previously confidential records. By aggregating data, or preventing the viewing of certain personally identifying fields, it is possible to render a database relatively innocuous whilst still maintaining its usefulness as an information resource.

3.6. Privacy Erosion

As noted, privacy is difficult to define and is a somewhat relative concept. Despite changes in what might be regarded as invasion of privacy over time, or in differing cultures, the erosion of privacy is a major concern [Macartney, 1988]. The fear is that small incremental erosions of personal privacy will go unnoticed or be tolerated. The likelihood of privacy erosion seems to be being kept in check at present due to the increased sensitivity of the general public "to the privacy implications of technological gadgetry and other forms of modern day intrusiveness" [Linden, 1988].

3.7. Existing Policies

As previously stated, freedom of information legislation contains various exemptions from the requirement to disclose government-held records. Privacy legislation in existence in many jurisdictions provides a different perspective on the protection of information privacy. One of the purposes of privacy legislation is to restrict the powers of governments to collect personal information about citizens in the first place [Mann, 1987]. It is also designed to regulate the use of such information once it has been collected [Flaherty, 1991].

Comprehensive privacy legislation has the following objectives:

- limitations on the collection of personal data;
- requirements that the data be relevant, accurate, timely;
- notice of the purpose for which the data is collected;
- limitations on disclosure without the consent of the subject;
- protection against unauthorized use of the data;
- open policies and practices;
- rights of the subject to review, challenge and correct data [Branscomb, 1986].

These objectives are, in effect, a summary of the basic principles of protection of privacy as established by the Organization for Economic Co-operation and Development [OECD, 1981]. Part two of the OECD Guidelines is located in Appendix I of this thesis.

The OECD principles, while only guidelines, have been adopted by many countries as the basis for privacy legislation. Guidelines such as these stipulate fair information practices by which custodians of personal data should abide [Flaherty, 1991]. These guidelines refer specifically to personal data.

"The threat to the right to be left alone is serious since only partial regulatory solutions have yet been achieved, especially for the private sector in North America" [Flaherty, 1988]. In Canada both freedom of information and privacy legislation only apply to government-held records [Privacy Commissioner of Canada, 1989]. In the U.S. many laws relating to access and privacy were prepared prior to the information technology revolution and so do not deal adequately with private sector, or integrated (compiled from more that one source), information. In many cases, if private sector databases are regulated, it is done pursuant to consumer protection legislation. In Canada a similar situation exists. A number of provinces have enacted Provincial Consumer Reporting

Acts, governing "the collection and use of information about private individuals which is intended to be sold to third parties" [Leia, 1989].

> The consciences of the collectors of personal information are all that control the uses of private-sector databases. Voluntary codes of fair information practices are visible evidence of ethical intent. Here there is some reason for encouragement .... But should one choose not to share one's own information with the marketplace, there is negligible protection in the now open season on personal information [Privacy Commissioner of Canada, 1990].

To address abuses that may occur in the dissemination of information in the private sector, the use of a privacy tort has been suggested. The tort of privacy was first propounded by Warren and Brandeis in 1890 and encompasses "an individual's claim against another who, in exercising an otherwise lawful right, impinges on that individual" [Halpern, 1990]. The application of such an approach would likely not affect public sector organizations, as they would still be regulated by existing freedom of information and privacy legislation. It would, however, place greater responsibility on private sector collectors and disseminators of information.

The issues of privacy and access to information, particularly as they apply to the private sector, do not appear to have been adequately addressed in North America. The Europeans on the other hand, through guidelines, such as those established by the OECD, provide for access and protection of personal data in relation to both the public and private sector [Leia, 1989]. Clearly, this second approach is more desirable. The practicality of a single set of policies and regulations is the most logical and least likely to fail due to claims of inconsistency and bias by one sector or the other. The right to privacy is something that must apply to all sectors of the community, not just to government . There is a need for privacy legislation that protects the right to information privacy of individuals over the whole spectrum of the information industry.

3.8. Privacy and Land Related Information

Although there is a large body of literature addressing the issue of privacy as it relates to personal information, such is not the case with land related information. This situation is a little surprising considering the amount of personal information often held as attribute data in land information databases. For land information systems, the major expenditure of effort up until quite recently, and still continuing to a large degree, has been the creation of digital databases. As the value of this information is recognized and it is utilized on a large

scale, the opportunities for abuse of this information will increase. What must be recognized is that at some point the supply of land related information will likely result in an invasion of privacy. To data there has been little detailed work addressing the issue of privacy as it relates to land information [ANZLIC, 1992].

Perhaps one of the reasons for the reluctance to recognize the threat of privacy invasion from land information is that the emphasis has traditionally been on the land component of the information, while the personal component has been regarded as subsidiary; necessary only for administrative purposes. To allow the efficient functioning of a land information system, there is a justifiable need for a certain amount of personal information to be collected, stored and used as an adjunct to the purely land related information. The intended use of the personal information provided must now be examined when questions of privacy arise.

A second reason often proffered to justify the neglect of privacy issues as they relate to land information is that much of this information is stored in public registries and must therefore be considered as public information not subject to privacy constraints. ANZLIC [1992] suggests that "a broad rule-of-thumb which can be adopted is that the continued provision of data/information which has been publicly available over a long period of time is deemed to have been accepted by the community at large as not violating privacy standards." The need to be conscious of privacy considerations, even for information made publicly available for statutory reasons or for the public good, is important especially in light of the increasing opportunities provided by computers to use such information for purposes other than originally intended.

Both of the above arguments come under considerable stress when the abilities of modern information technology are considered. In our modern society where the qualities of economy and effectiveness often dictate that organizations share data resources, there is great potential for privacy invasion. The collection of information from multiple jurisdictions and its selective merger has the potential to create personally intrusive information from land related information.

Part of the problem is in recognizing just where the line between land related information and personal information should be drawn. There is also a need to discern when the use of an ostensibly land information database ceases to have its main emphasis on land information and instead is used to produce information that has personal information as its principle theme. It is important to maintain the correct perspective or balance. Protection of privacy should not prevent the legitimate use of information. Disclosure of personal information does not necessarily precipitate a breach of privacy. As

noted by the Australian Senate Standing Committee on Legal and Constitutional Affairs [1987], "it is desirable to safeguard private information about individuals; but it is not necessary to prevent the circulation of all information about identifiable persons." The protection of personal data is not the issue. The issue is the protection of privacy [ANZLIC, 1992]. When attempting to foresee whether land information and its attendant personal information can be released without causing an invasion of privacy, consideration must be given to the current values of the community, the intended use of the information and the capabilities of technology.

4. Influencing Factors

Access and privacy cannot be addressed in isolation. They are part of a complex web of institutional issues which are encountered in the use of land related information. All of the issues expanded upon below impact to some degree on access and privacy.

Many government agencies are being encouraged to take a more commercial attitude towards marketing their considerable information holdings. Such a position is primarily being developed due to the realization of the revenue producing capabilities of information. In conflict with this approach is the view that information gathered by government is funded out of the taxpayers' pocket and so should be freely available, as a public benefit, to all members of the community.

This second stated, traditional, view is being challenged by:

- pressure to increase income from external sources;
- widespread application of the user-pays principle to government services;
- a demand from governments that valuable assets be fully exploited;
- pressure from the private sector to gain access to valuable land information held within government databases [ALIC, 1990d].

Information gathered by governments over the years has great value to all members of society. "This value is being recognized by an increasing proportion of private sector firms and other governments and data is already being distributed in a variety of ways, under a variety of pricing structures, with no overall pricing or distribution policy in force" [Land Information Steering Committee, 1990]. The basic competing forces in the distribution and pricing debate are those of public benefit and commercialization.

Public benefit may be defined as "the use of public funds to provide services to the community" [ALIC, 1990d]. These services generally fall into the category of being in the public interest or essential in nature. Factors such as cost, accessibility and availability have a large influence on this social value of information [ALIC, 1990e].

The contrasting view to public benefit is that of commercialization. The principal motives behind commercialization are to "increase efficiency, rationalize the demand for both products and services and to increase revenue" [ALIC, 1990d]. As far as the private sector is concerned, commercialization means deriving a profit to facilitate the continuation

of business activities. For the public sector, commercialization may relate to profit seeking, or alternatively to partial or full cost recovery.

The contentious issues of distribution and pricing are both strongly influenced by arguments relating to public benefit and commercialization. Debate surrounding distribution and pricing also recognizes the critical role that ownership of information plays. When applied to digitally stored information, and all the possibilities that follow, determining ownership becomes a very complex issue. Liability, by comparison, remains relatively unchanged by the advent of electronic information. All of these factors, as will be shown at the conclusion of this chapter, colour any policy that addresses access and policy.

4.1. Distribution

Information may be supplied by public means, private means, or any one of a broad continuum of hybrid means that lie somewhere in between. Ultimately the balance of responsibilities between the public and private sectors depends upon:

1. the nature and traditions of the particular jurisdiction;
2. specific information needs and priorities;
3. the available funding;
4. questions of access to the data and the need for privacy;
5. the initiative shown by the private sector [Dale and McLaughlin, 1988].

As the above list implies, the method of delivery of information is dependant upon the expectations, rights and obligations of both the supplier and the people requesting the information. These expectations, rights and obligations have two basic dimensions when the choice between public and private delivery is offered:

1. financing — should we pay for some good or service individually, out of our own resources, or should we pay for it collectively with funds raised through one form or another of taxation?
2. performance — should the good be produced or the service delivered by a governmental organization or a non-governmental organization? [Donahue, 1989]

This statement of the issues can be illustrated by the matrix shown in figure 2.

	Collective Payment	Individual Payment
Public Sector Delivery	"Government" - education - police - national defense	- postal service - admission fees to govt. parks - fees for launching private communication satellites
Private Sector Delivery	- police patrol cars - stationery the govt. purchases - services of consultants to govt.	"Private Sector" only govt. involvement is in regulating, monitoring and certifying private exchange

Fig. 2. Dimensions of the Private/Public Choice (after Donahue [1989, p. 7])

4.1.1. Distribution Mechanisms

The bulk of land information is held by government agencies, but they may not necessarily wish to be responsible for its distribution. If the public sector does choose to disseminate the information by its own means this does not ipso facto mean that government sees itself as an entrepreneur. The government may see itself purely as a provider of public services for the good of society [Kozub, 1991]. A choice must be made as to the degree of 'publicness' or 'privateness' desired of the organizations charged with dissemination of any given information product. The range of organizations capable of information management and dissemination include:

- departments wholly controlled by government;
- semi-autonomous government corporations;
- local government;
- private non-profit organizations;
- private business.

The benefit of government marketing its own information is that a large degree of control can be maintained over the information and the distribution process. Detracting from this is that the task of carrying out the mainstream objectives of the government is difficult enough as it is, and any distractions should be kept to a minimum [CLIC, 1991].

The approach traditionally adopted by the U.S. is to enlist the help of the private sector "to improve the performance of tasks that would remain in some sense public" [Donahue, 1989]. The advantages of disseminating government information through the private sector are as follows:

- department operations benefit by
  - increasing productivity
  - reducing overall costs
  - improving services to the public
  - allowing better management of information holdings;
- the development of a more viable ... [private] industry is assisted;
- access by all ... to essential information held by government is enhanced;
- access by industries wishing to provide further value-added services is enhanced [Land Information Steering Committee, 1990].

An example of the range of distribution mechanisms that may be adopted by government is found in the following list:

1. ministries each distribute their own data to customers;
2. data from all ministries is distributed via a single value-added agency to all customers;
3. data is distributed by multiple value-added agencies, each responding to a specific market;
4. data is distributed by multiple value-added agencies, each dealing with specific data;
5. a data utility providing a link between producing ministries and value-added agencies [Land Information Steering Committee, 1990].

4.1.2. Wholesaling and Retailing

Just as traditional goods may be traded at the wholesale or retail level, so can information. The release of information which contains a significant value-added component is called retailing, while wholesaling refers to the release of information in its raw, or only slightly value-added, form [Perritt, 1990].

ACUS [1989] defines retailing as

> providing information in a format different from that used by the government, or with accompanying analysis, aggregation or segregated subsets, enhanced search or retrieval capabilities, or otherwise tailored to be of value to specialized or individual end users; also may include distribution components of electronic release.

Wholesaling is defined as "providing resellers or large end users information only in the form used by the government or only in bulk form."

It would seem logical that government should restrict its sale of information to the wholesale level, while leaving retailing to the private sector. It is inevitable, however, that at some stage value will be 'manufactured' by government. Significant value adding in the form of data structure, indices, and search and retrieval software will likely result as a by-product of internal automation of government. This activity may be a legitimate response to aid in fulfilling the legislated mandate of an agency.

> The policy challenge is to determine when it is most cost effective for the government to disseminate value already added for its own internal use, to add additional value solely to meet public demand, or to rely on the private sector to add value [Perritt, 1990].

4.1.3. Private Sector Efficiency

At times the opinion that the private sector can provide products or services cheaper or more efficiently than the public sector is proffered. Such assertions are often made with no real justification or substantiated evidence. While the private sector may be able to meet the needs of an information hungry society 'better' than the public sector, documented cases indicate that the private sector is not always the more efficient of the two [Donahue, 1989].

Many studies have been carried out to compare the provision of certain services by both the private and public sector. Depending on the form of private organization and the type of service being studied, the results differ. For example, in the provision of such utilities as power or sanitation, the public sector has been shown to be on a par, or even cheaper, than a private sector organization providing the same service. Other tasks which have been studied show that the private sector is overwhelmingly more economical at providing the service [Donahue, 1989].

The manner in which the private sector is deployed in any given task would appear to have some bearing on the benefits to be gained. Donahue [1989] enunciates three common means of applying the private sector to a task:

- contract – a large (government) organization contracts with a private organization for the provision of services;
- franchise – a single private sector organization is authorized to provide services in a particular area, but is paid on a piece-meal basis by the individuals who use the service within that area;

- competitive – individuals make their own arrangements with separate companies for the provision of services.

Not all of these are appropriate for the provision of information services. It is important to note that there are wide disparities in the efficiency effected by each of these groups in any given circumstance. What is most efficient for one task may not be the most efficient for another task. For example, over zealous application of the competitive approach may lead to fragmentation of the market [CLIC, 1991; Donahue, 1989]. Such fragmentation may be detrimental, resulting in low profits for all distributors and expensive access for users.

In most industries competition has been demonstrated to benefit customers. Given a large enough market, competition in the provision of services, whether by private or public means, breeds efficiency. Studies have shown that government efficiency will increase to the point that it is on a par with the private sector if it is required to compete on equal terms. Equally, if there is no real competition, even the private sector will become lax and fail to provide services at an efficient level [Donahue, 1989].

4.1.4. Selection Criteria

The distribution route selected in any given case will depend on many variables. Three key variables considered when government determines whether to use its own resources or to rely on the private sector to disseminate information are: control, expertise, and economics [CLIC, 1991]. Some tasks are best left to the government, while others are achieved with greater efficiency by the private sector. Factors likely have a strong impact on the option chosen include:

- the degree to which a task can be precisely specified in advance;
- the ease with which the value of production can be assessed (i.e. the measure of productivity);
- the ease with which a person or organization may be replaced (or otherwise penalized) if their work does not reach certain standards;
- the level of expertise that the principal organization has with regard to the means of accomplishing a given task;
- the relative importance of ends and means to the completion of a task [Donahue, 1989].

The initiative shown by the private sector will also be critical in determining the distribution method. If the actions of the private sector clearly demonstrate their competency to carry out the task, and their efficiency can be proven, government will have little choice but to adhere to the dictates of the market. The only factor that may act to retard this shift of activity is concern for public benefit principles such as protection of privacy and access. The private sector may find adherence to such principles too onerous or too uneconomical if a healthy and financially stable business is to be maintained [CLIC, 1991]. Nevertheless, the combined application of sound business principles and public benefit is necessary if the greatest advantage, for the community as a whole, is to be derived from the use of information.

The most likely scenario is that the combined efforts of the public and private sectors will provide the best solution in many situations. Rather than being viewed as competitors, the two sectors should see each other as being complementary: both having strengths and weaknesses. The harnessing of the best of both approaches will lead to the effective management and use of information and the greatest chance of beneficial utilization of a valuable resource [Perritt, 1990].

> To date government agencies have been the traditional repositories for the majority of land related data, while the private sector has taken the entrepreneurial role of using data for commercially viable activities. Governments, the private sector and individual users must continue to promote interaction to ensure the wider use of all land related data, recognising that the skills within these sectors are complimentary... [ALIC, 1990e].

4.2. Pricing

Questions such as who should distribute information, how it should be distributed, and, especially when government is involved, what pricing strategy should be employed, are all contentious discussion items. The arguments explored in this section will centre mainly on government agencies and government-held information. The private sector is not as hamstrung as the public sector. Its attitude regarding information and pricing strategies related to the supply of information, as with all things, is largely driven by market forces. The public sector on the other hand has a more complex and conflicting set of principles to bear in mind. In the area of pricing, two extremes that have developed are the 'give-it-to-them-at-cost' approach and the 'charge-the-buggers' approach [Lawrence, 1990].

The 'at-cost' school argues the following case:

- the data was collected at the taxpayers' expense and is therefore public information and should be readily and cheaply available;
- if users are required to pay for the information, there is in fact double taxation taking place, as those same users are required to pay for its collection in the first place, through taxes.
- 'purse string' regulation will effectively curtail equity of access for all citizens;
- information availability at a unilaterally low price is good for society as a whole, as it has the potential to stimulate the economy through the activities of entrepreneurs;
- the commercial use of data, and subsequent information, collected by government must be secondary to the mandated use of that information, as such the bulk of the cost should be absorbed by government rather than being foisted upon private citizens.

The 'charge' school argues that:

- those who use the information and benefit from it should pay for the information, rather than those members of the public who do not use the data;
- the individuals or companies that want the data are likely to use it for some commercial purpose, and so should be charged a realistic price for it;
- the provision of information requires a great deal of capital investment – if charges are not levied to enable information suppliers to recoup their expenses, the information will probably not be provided at all;
- by charging for use of the information, revenue can be generated and used to provide more and better information services;
- government agencies are in possession of information which has value far beyond that for which it was originally collected – the additional processing required to compile the information satisfactorily for external use is justification for a user fee.

There are many questions that need to be addressed as governments move away from the traditional approach of providing data at a token price. Apart from matters relating to how the information will be distributed, the following questions about what constitutes a reasonable, justifiable or appropriate fee must be dealt with:

1. who should pay for land information products and how much;
2. whether all front-end costs, such as establishment of geodetic control, should be recovered through fees;

3. what should be the contribution from general revenues and what from special taxes;
4. what is the case, if any, for price discrimination between different users and different products [Dale and McLaughlin, 1988].

4.2.1. Justification for Charging

There may be many good reasons for governments to continue providing non-confidential government-held information to the public at token cost, but more and more, governments are turning from the token cost approach to the fee charging approach. Some of the justifications for governments charging users for information are:

- to seek a return on the government's investment in collecting and maintaining the land-related data;
- to cover organisational costs in the provision of land information products and services;
- to increase efficiency in the allocation of resources within organisations;
- to enable market forces to influence demand and supply of land information products and services;
- to keep government costs in distribution to a minimum by discouraging unnecessary use of land information services (i.e. to ration excesses);
- to generate income to support the expansion of services and thereby encourage service growth;
- to provide an incentive for the use of spare capacity by enabling agencies to generate and utilise additional revenues [ALIC, 1990c].

4.2.2. Cost Recovery Options

Dale and McLaughlin [1988] cite three basic strategies for price determination:

- cost based pricing;
- demand based pricing;
- competition based pricing.

The Land Information Steering Committee [1990] of British Columbia expands on this list and specify what they consider to be the five most common cost recovery options. Comments on the suitability of each option, from a government perspective, are also offered.

- Incremental cost recovery – represents a minimum charge which corresponds to the cost which would not have been incurred had the product not been sold. This approach is not recommended.
- Direct cost recovery – involves recovering direct costs such as labour, materials, etc., but not indirect cost such as capital and overheads. It is not recommended as it bears no real logic in the allocation and identification of costs and will likely result in inconsistent pricing of products supplied on different media.
- Partial cost recovery – (see definition in section 4.2.3.) This option offers a logical and defensible approach with the necessary degree of flexibility to meet both market and political considerations.
- Market value pricing – the price of the information product is determined on the basis of supply and demand. This approach is usually adopted when the product is competing directly with an equivalent private sector product. In theory this is the most attractive option, however, for most types of government land related information no equivalent private sector product exists and no price has been established in the market as yet.
- Full cost recovery – involves recouping capital costs (e.g. hardware; software; telecommunications; project development and administration; data collection, preparation, correction and updating; data conversion; documentation; training; marketing; etc.). This approach is not recommended for a number reasons. Firstly, the systems were designed originally for government use and to attempt to recover their full costs would be inappropriate. Secondly, if the price reflected the full capital costs of assembling the databases it would in most cases be far too high to attract users.

4.2.3. Partial Cost Recovery Model

The potential of revenue generation from the sale of information is considerable [ALIC, 1990e], however, restrictive policies could inhibit the realization of substantial gains. Any pricing policy should recognize the benefits to be had as well as the requirement to be mindful of the need for a public benefit component in the supply of information. The B.C. Land Information Steering Committee [1990] gives the following definition of a partial cost recovery model.

> The objective of the partial cost recovery model is to charge users with a fair proportion of the total costs of the service which at a

> minimum reflects the incremental costs of providing the service and at the maximum reflects the market's view of the value of the service.
>
> The general principle of the approach requires that customers, as a group, pay a share of the following costs:
>
> 1. a capital cost component reflecting the costs of creating the database, amortised over the life cycle of the database;
>
> 2. an operating cost component, reflecting the ongoing costs of maintaining and updating the database; and
>
> 3. an incremental cost component reflecting the costs of providing the service or product which would not be incurred if it were not sold.
>
> The share of the capital and operating costs assigned to the user group may vary between 0% and 100%. The share of the incremental costs assigned to users should always be 100%...

Such an arrangement appears both fair and flexible. In the event that it is felt that information should be provided at a nominal cost, this model is equipped to handle that desire. It is equally well equipped to respond to a more commercial approach to the provision of information. As more information products become available on the market from private sector sources, the government charge for similar information can be altered within the terms of this model. The only restriction created by this model is that there is no provision for a profit margin. This is quite acceptable, as the model is designed for cost recovery, not profit making. This is probably the approach that should be taken to avoid undue aggravation of the private sector.

4.2.4. Discretionary Pricing

In the ideal situation, the pricing policy for information would be the same for all parties. In reality, a single hard and fast pricing structure cannot easily be applied. If exceptions to the standard price for a particular product or service are to exist, they should at least be kept to a minimum. The proliferation of different rates for the same product are complicated to implement and difficult to monitor and will inevitably give rise to claims of inconsistency, bias or favouritism [CLIC, 1991].

Wherever possible, differences in price for a particular product or service should be justified within the bounds of the pricing policy adopted. It is likely, however, that there will always be cause for cost inconsistency. Charges are likely to be varied due to such matters as:

- the volume of data supplied;

- precedent;
- product form;
- whether the intended use of the information is to be for the public benefit or for profit;
- statutory charges or requirements;
- legislative arrangements;
- reciprocal arrangements for data exchange between data custodians;
- reciprocal arrangements with users arising from joint development of products or systems;
- market value [ALIC, 1990c].

4.2.5. Balanced Pricing Policy

The fundamental questions posed to all government entities contemplating and currently involved in selling information products are:

- what to charge for;
- who to charge;
- how much.

As with most things, there must be some compromise, some recognition of opposing arguments. In this case, a balance must be created between public benefit and commercialization. Users fees may need to be charged to ensure the continued supply of information to the public but at the same time pricing must not be used to restrict access to information. Commercially biased policies may result in a society which is divided into groups which are information-rich, because they can bear the price, and those that are information-poor [Davies and Lyons, 1991].

The mandate of each agency will be a key factor in the cost recovery debate. The mandate will determine whether an agency can default to user-pays principles, or whether it is charged with an over-riding duty to inform the public. In establishing government mandates and generating policy statements the outcome will be dependant upon social, economic and political factors.

4.3. Ownership of Information

The realization of the commercial value of information depends, in large measure, on the ability to control its use. That control can only be justified if a claim of ownership can be proved.

The growing socio-economic importance of information and its handling, especially in more technologically progressive societies, is self evident. It is predicted by many that the information revolution currently under way may prove to be the most world transforming of any of the successive large scale society altering revolutions to date. The broadening use of information technology has perpetuated the realization that economic activity is to a large extent dependent upon the generation, storage, retrieval, processing, transmission and use of information [Economic Council of Canada, 1971]. Recognition of proprietary rights is an important step toward ensuring that creators of information are acknowledged and rewarded on a level commensurate with the product's value to society. If trade in information is regarded as a legitimate business activity, worthy of remuneration, then what of the owners of data? If data and subsequent information is of value, should the owner have the right to authorize its sale and collect some recompense upon its use by third parties? The issue of recognizing information as property and understanding the proprietary relationship attached is something that has received little attention to date [Branscomb, 1986].

4.3.1. Intellectual Property Rights

Within developed countries, intellectual property is a marketable commodity. An information society places economic value on intellectual property and derives some part of its wealth from its use [Branscomb, 1986].

"Intellectual property rights ... are the means by which ideas and technologies at the cutting edge of progress are protected and further innovation encouraged" [Science Council of Canada, 1990]. The major means of protecting intellectual property are copyright, patents, trademarks, trade secrets and industrial designs. It is copyright , patents and trade secrets that are most applicable to computer programs and, of greater interest to this study, information.

4.3.1.1. Patents

Upon the filing of an application and the successful granting of letters patent, a statutory monopoly is granted to the inventor of "any new and useful art, process, machine, manufacture or composition of matter, or any new and useful improvement..." [Canadian Patent Act, 1970]. A patent can not be issued "for any mere scientific principle or abstract theorem" [Canadian Patent Act, 1970].

Patents are used to protect the entire inventive concept of a particular idea and in addition can be used as protection against somebody else inventing the same product

independently. This philosophy is in contrast to copyright laws which only protect the expression of the idea, not the idea itself, thereby allowing another party to develop a similar product, so long as they do so by their own independent efforts [Mann, 1987].

4.3.1.2. Trade Secrets

The common law protection of trade secrets represents perhaps the best form of protection of information. Using trade secrecy laws, information itself may be protected, unlike the protection offered by both patent and copyright laws.

There are two conditions which must be met for protection of information to be offered under trade secrecy laws. Firstly, the information must be confidential rather than a matter of common or public knowledge. Secondly, any party who receives the information must keep it confidential [Mann, 1987]. Both of these conditions impinge heavily on the reasons for wanting to protect the ownership of land information.

4.3.1.3. Protection and Use of Information

As information providers, greatest commercial benefit is generally obtained if a large market is reached. While a large market is desired, the control of the information is also desired, if only to restrict its use by parties who have not paid for it.

The use of trade secrecy laws defeat the purpose of being an information provider. It is necessary for the market to know of the availability of the information, and to use it, if the provider is to gain a return from its existence. Patent law, likewise, is likely not the best means of protecting ownership rights in information. The patent route can be very expensive and time consuming and, more importantly, has not been used effectively for protecting computer programs and other computer related subject matter (i.e. information compilations) [Mann, 1987]. Copyright law, although not ideal, seems to offer the best option as far as protecting the rights of information holders while at the same time allowing information to be used by a specific client group.

4.3.2. Copyright

To ensure availability of information while at the same time protecting the provider from its misuse, it is necessary to exercise some form of ownership right. This right is best protected by copyright. "Copyright law is the legal recognition of the right of creators. Its purpose is to protect the results of intellectual and creative labour" [Department of Communications, 1984]. This definition sits very well with the concepts of data and information. A person may be in possession of some raw facts, or data, but the party that

takes those facts and performs some operation on them to produce useful information is the person who should benefit from the protection afforded by copyright.

Section 3(1) of the Canadian Copyright Act [1985] defines copyright as "the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever." As far as land information is concerned, there are two formats of work that are likely to be protected by copyright: artistic works and literary works. Artistic works include paintings, drawings, maps, charts, plans, photographs, engravings, sculptures, works of artistic craftsmanship and architectural works of art. Literary works include tables, compilations, translations and computer programs.

Two fundamental principles of copyright are that ownership of copyright does not necessarily follow physical ownership of the work, and that only the form of expression of the work is protected, not the idea, concept or subject matter of the work. Copyright affords a narrower protection of rights than a patent in that it only provides for protection against copying, not against independent creation [Burshtein, 1987].

While facts cannot be copyrighted, compilations of facts can be [Dando, 1991]. Databases, being compilations of facts may be copyrighted. What is protected, however, is the specific presentation of the data, not the data, nor the facts themselves.

Copyright cannot subsist in any work until that work is produced in some tangible form. The work must exist in some form susceptible to being copied. This is one of the weaknesses of copyright. As with most legislation currently in existence, the protection is directed more toward the physical manifestation and the medium, than the information itself.

The ownership of copyright can become very difficult to determine, especially when digital information and compilations of digital information are considered. Legislation has not yet been developed which effectively deals with issues which have been brought upon us by breath-taking advances in technology.

When the author of a work, who is being compensated by a second party for time and resources expended, concludes his or her labour, the ownership of that work, and the copyright in it, will be determined by considering whether the author prepared the work under a contract of service, or a contract for services. If the author is under a contract of service there is no doubt that the ownership of the copyright belongs to the person or organization for whom the author was working. An independent consultant, however, may be under a contract for services. In such a case, the ownership of the work, in the absence of an agreement to the contrary, may be retained by the consultant [ALIC, 1990b].

An example of land related information that may be subject to confusion as to ownership is the production of a plan of survey by a surveyor. In providing a plan to a client, unless explicitly stated, the surveyor is not transferring the copyright, but simply providing an implied licence to use the plan for its intended purpose [Penfound, 1990]. Use of the plan may include making copies to facilitate approval by various authorities, or registration of the plan as a public document. When copies of a plan are made which can reasonably be said to fall within the intended use of the plan, copyright is not infringed.

In the event that a plan of survey is registered as a public document, and this intention was clear from the outset, the use of the plan by the Crown would appear to be legitimate [Penfound, 1990]. Although copyright may remain with the surveyor, an implied licence is granted to the Crown to use that plan for the public good. Such public good may include resale of the plan to the public and the production of maps using information from the plan.

At what stage does the use of information from a plan, to produce a map, constitute a breach of copyright? The message in the following statement represents a common opinion regarding compilations. If sufficient effort has gone into creating a new database, copyright has not been breached.

> Where data entered into public or private sector agency data bases has been derived from a range of documents, and employees have applied a significant measure of skill, ingenuity, experience and labour to originate a new product (a computer-based land information data base), there is considerable justification for a claim that these bases are literary works within the context of the Copyright Act and that the copyright which subsists in them is vested in the constructing agency [ALIC, 1990b].

Mann [1987] states that a compilation of data submitted by various authors should be considered a collective work. In such a situation, copyright may subsist in the compilation as a whole and be owned by the author of the compilation. At the same time, copyright may be retained for the separate components by the authors of those components. For a compilation of separate works to exist and for copyright to subsist in the compilation as a whole, it may be necessary for the author of the compilation to gain permission from the individual authors for the use of the individual components.

A further nuance is encountered when information is submitted to government in electronic or digital form. In this case the amount of skill, ingenuity and labour employed to create the compilation may be significantly decreased. In such a case the ownership of

copyright is very much open to question. It is likely that copyright will not subsist in the new database [ALIC, 1990b].

Dando [1991] reports on a recent case decided by the U.S. Supreme Court which clarifies some points in the area of copyright. The court held that facts may be freely copied without infringing copyright. This is a shift from the previous stance that each creator of a work must gather the facts from the original source. The two principles used in the case were:

- facts are not able to be copyrighted;
- only the selection, coordination and arrangement of facts may be copyrighted.

This court ruling, if applied to land information, often represented in the form of a map or plan (digital or hardcopy), suggests that if the facts have been gathered from other existing maps or plans, but the same selection or arrangement has not been used in the presentation of the compilation then copyright has not been infringed.

4.3.3. Custodianship

Custodianship is a term often associated with ownership, however, the two are quite different. Custodianship is the collection and management of data by an organization or part of an organization on behalf of the wider community or the larger organization. The data is not owned by the custodian, but held in an attempt to provide effective management of the data. The custodian is subject to certain responsibilities with respect to the data and is entitled to certain rights [ALIC, 1990a]. Custodianship (or trusteeship) is a term used when dealing with a corporate information resource.

Data custodians are responsible for the processes and functions of data capture, validation and maintenance, including principles and procedures for accuracy, currency, data storage (definition and structure) and security. The requirements of all users need to be assessed and actively taken into consideration by the custodian. In return for the services provided, the custodian is entitled to charge users for use of the data, may license users and distributors of the data, and may market such data in much the same way as an owner would [ALIC, 1990a].

Selection criteria for custodians include:

- the agency which has sole statutory responsibility for the capture and maintenance of the data item;
- the agency which has the greatest operational need for the data item;
- the agency which is the first to record changes to the data item;

- the agency which is the most competent to capture and/or maintain the data item;
- the agency which has the confidence of users that it will continue to meet its commitments to data collection and maintenance;
- the agency which is in the best economic position to collect data at its source;
- the agency requiring the highest integrity of the data item [ALIC, 1990a].

Difficulties in the use of the custodianship model may arise due to:

- data management priorities of trustees might differ from priorities of the LIS integrator;
- data quality needs of trustees differ from those of an integrated system;
- trustees are not always keen (because of tradition or lack of funding) or able (because of lack of skills) to change long standing data (mis)management procedures;
- agencies, through being trustees, assume greater than warranted management control over the integrated LIM function;
- agencies will protect their own interests and business objectives from what they might consider undue intrusion or competition [Hart, 1991].

To control the use of information it is advisable that a contractual agreement be reached prior to the supply of the product specifying the terms and conditions under which it may be used. The use of information for the creation and sale of value added products is also best controlled by licensing agreements, rather than relying on copyright. A value added product may be sold to a third party, but it is imperative that the creator of the original information be in a position to gain proper compensation for its use.

"Royalty is the monetary consideration received by the owner of copyright in a work from a person for a licence to make copies of that work" [ALIC, 1990b]. The term Royalty, due to its meaning of 'licence to copy', may be inappropriate, especially for digital data. The term licence fee more accurately describes the transaction that is likely to satisfy the custodian's or owner's continued desire for control over the information. The licence fee may include a contribution towards the cost of creation of the product, the total labour and material costs required to service the users request, and a margin of profit. By issuing a licence to use information, an owner is not selling the proprietary rights to that information, but permitting the use of the information for a particular purpose and duration

as specified in the contract created to effect the sale. In the case of a custodian, a licensing agreement enables the maintenance of an appropriate level of control over the data.

In determining the licence fee, consideration must be paid not only to the highest value of the information, but also to the best use of the information. Data collected and information created by government organizations is often justified in terms of benefits for the public good. If the public good is not to be compromised, information may have to be supplied at a cost which can not be justified on a wholly commercial basis.

The following terms and conditions should be included in any agreement or licence:

- the requirement for a licence fee (or other form of consideration);
- term (time period) of data delivery;
- intellectual property indemnity;
- limitation of liability;
- disclaimers and release;
- confidentiality of information between department and client;
- verification of proper data use;
- security and control of data in the licensee's control;
- indemnity for modifications by the licensee;
- data update;
- schedules, which include statements about the equipment needed to use the data, the format of the data, the storage media, and other documentation [ALIC 1990b].

4.3.4. Summary

Problems arise when trying to determine if ownership rights, or copyright, have been infringed. This is particularly so with electronically stored information. Is the creation of a value added product the formation of new information? What of the case where old information is simply reformatted and presented in a manner which makes a clearer statement of a message to a particular user? What of the practice of combining several different pieces of information to communicate a message? Copyright may not be violated in such a case, but are the owners of the separate information elements entitled to some form of recognition? It would seem that the maintenance of the original linkages between source data (the presentation of the facts in the initial work) plays an important role in determining if a new product has been created [ALIC, 1990b]. These and other questions

that arise out of the use of a technology that places vast amounts of processing power at our fingertips have not been adequately addressed by users or policy makers.

Custodianship, which can apply equally to public and private sector organizations, and even to arrangements which involve cooperation across the sectors, is particularly relevant when dealing with corporate data. The benefits to be gained, such as increased integrity and decreased duplication are necessary for the expansion of efficient and effective information systems.

Copyright law appears to offer the best alternative for the protection of information. It is the best option available to control access and quality of information [CLIC, 1991]. It does not, however, address some of the issues that have developed in recent years as a result of the use of information technology. The application of laws to problems for which they are not particularly suited is less than ideal. There is a requirement for policies and legislation that explicitly recognize the value and issues associated with information itself, rather than the medium on which the information is located.

The use of copyright alone is unlikely to provide an acceptable level of control over information. This is particularly true when databases are compiled from a variety of sources. Under existing conditions, the most effective means of bridging any gap is to make use of contractual agreements to clarify any areas of doubt.

4.4. Liability

The provision of land related data or information exposes the provider to liability for the costs incurred by the user as a result of inaccuracies in the data or information [Chatterton and Epstein, 1984]. The issue of liability is never far from the information provider's mind, especially in today's litigious climate. In a legal sense, there are two means by which liability claims may arise:

- breach of contract;
- negligence (in tort).

In the area of negligence there are four elements which must be proven to establish that negligence exists and that the wronged party (plaintiff) is entitled to recover damages:

1. the supplier of information (the defendant) owed the plaintiff a duty of care to protect the plaintiff from injury;
2. the defendant breached that duty by acting improperly or failing to act at all;
3. the defendant's breach caused the plaintiff injury;

4. the damage to the plaintiff was foreseeable to the defendant [Alberta Land Surveyors' Association, 1991].

Contractual liability issues are more clear-cut than liability based in tort [Salmon, 1989]. Written contracts ideally promote communication between the purchaser and the supplier, resulting in the formal allocation and declaration of the duties and responsibilities between the parties.

Even though contracts offer a relatively straight forward means of explicitly stating the responsibilities of all parties involved, information systems in both the private and public sector seldom use contracts resulting from negotiation between the parties [Epstein and Roitman, 1987]. Perhaps the perception of information systems as being spontaneous, timely and flexible contributes to the reality that negotiated contracts are seldom seen as appropriate. Where information is shared between government agencies a Memorandum of Understanding is often used rather than a contract in an attempt to clearly state the responsibilities of the parties involved [Salmon, 1989].

The use of modern technology increases the exposure to liability of any information system and its operators. Increasing client bases, both in numbers and types of users, mean that the information is being used more often for an ever expanding variety of tasks. As the number and type of applications and users increases, the potential for errors to be discovered and damages to result will increase. Means of effectively reducing or minimizing liability are of great importance in any commercial setting.

4.4.1. Duty of Care and Third Party Liability

A duty of care may be owed when a person knows that others will base their activities on the assumption that the information supplied to them is correct. This duty of care, originally only applicable to professional people and their direct clients and employees, has now been expanded to apply to any information provider. The duty of care is owed to all people, or class of people, who might reasonably be expected to rely on the information.

The expanded duty of care results in liability not being restricted to immediate clients, but extending to a much broader class of people, including third parties. There now exists a solid legal basis, in common law countries, upon which to find third party liability on the part of information providers [Campbell, 1980]. In order to prove that an information provider is liable to a third party, the following questions must be answered:

- did the information provider breach the standard of care expected of a person in that position?

- is the plaintiff a member of the class of persons to whom the defendant owes a duty of care?
- was the plaintiff's reliance on the information reasonable in the circumstances?
- did the plaintiff's reliance on the information result in damages? [Campbell, 1980]

In any discussion of this topic, the word 'reasonable' continually arises. For instance, courts have remained conscious of the need for reasonable limitations on the scope of the class of persons who can claim a duty of care is owed to them [Sookman, 1989], and damage incurred must have been reasonably foreseeable to the defendant. The area of liability can at times seem very subjective in its determination of what constitutes reasonable activities, reasonable precautions and a reasonable person.

4.4.2. Limiting Liability

When it comes to limiting liability, the ideal option would be to produce information which contains no errors and cannot be misused in any way. Such a scenario is likely to be impossible to achieve. The best to be hoped for is to bring the number of errors in the information to a minimum, or to reduce their number to an acceptable level.

Epstein and Roitman [1987], and Salmon [1989] have suggested several activities that can be used to diminish the risk of liability.

- Computer hardware and software must be carefully selected and the system well maintained. The system must be able to adequately carry out the tasks which its owners and operators promote it as being capable of performing.
- The quality of data in the database must be good enough to support the level of decision targeted. Details on timeliness, mapping scales, completeness, precision, source of data, context of collection, etc., must be made available to ensure the user is able to determine if the quantity and quality of data is sufficient to produce a product which can be relied upon in the decision making process.
- Data entry techniques must be adequate. Data entry techniques must be developed which result in an acceptably low level of errors. Processes for data verification and cross-checking of data will aid in the achievement of this goal. Processes for error correction must also be in place.
- Analysis of the uses of the data in the system must be carried out. Data and functions available on the system may be used incorrectly, either deliberately or accidentally. Careful analysis of all the tasks the system can perform, and how

those tasks could adversely affect people must be carried out. Issues that may have to be included in such a study include:

a) the system may operate at an acceptable level of error for internal use, but produce an unacceptable level of error when used externally;

b) the system must produce information that is difficult to misinterpret. Meaningful results must be the norm. The system and data should ideally be used only for the purposes for which it was designed.

- Security concerns must be considered, especially for on-line systems. Protection of personal and proprietary information is vital. Access to the system by clients (private or public agencies) should ideally be controlled by contractual arrangements. Features such as passwords and limitations on read and write permissions should be standard.

A number of additional points to be remembered when talking about liability are:

- limitation periods, which state the maximum time which an individual can be held accountable for inadequate products or services, may commence not from the time the mistake was made, but from the time the error was discovered and damage suffered [Penfound, 1990].
- computer error is not a defense against negligence. An information system must be at least as efficient and error free as the manual system it replaces [Epstein and Roitman, 1987].
- information providers should foresee that the system will at some stage go down or fail. If there is no contingency plan, loss or damage may be suffered by those relying on the system. Reasonable steps must be taken to avoid this occurrence [Sookman, 1989].

The use of contracts is the preferred means to limit liability. They can be used not only to state the rights and obligations of each party, but also to discourage the unauthorized use of information and information products and thereby limit third party liability. The use of contracts and standard disclaimers are necessary in today's business environment to limit exposure to liability [Sookman, 1989].

The Alberta Land Surveyors' Association [1991] notes that Ramsay has suggested the following as a means of limiting the 'fall-out' should the possibility of legal action against an information provider be likely:

1. contractual limitation;
2. risk of use transferred over to the user;
3. use warnings;
4. acceptance testing;
5. taking reasonable measures to avoid errors;
6. use of liability insurance.

4.4.3. Summary

To prevent excessive losses from legal action as the result of negligence, it is necessary for the information provider to provide an adequate or reasonable standard of care in all cases. With each case the standard will vary, although there must always be some minimum requirement. The standard will be governed by such factors as:

- the type of information made available;
- the importance of the information;
- the uses to which it will likely be put;
- the cost and practicality of providing 'error free' information;
- who has compiled the information;
- the common practices of others in the business;
- the reliability of the manual system which the computerized system is designed to replace [Sookman, 1989].

Competent and complete performance of the required work is the best means of limiting liability. The fewer errors in existence, the smaller the likelihood that those errors will result in damages to a user. Quality control procedures designed to detect and allow for the correction of all but an acceptable level of errors before the data is available to the general user are critical [Onsrud, 1990].

Information suppliers can try to ensure that an adequate standard of care is given to all products for which they are responsible, but in the end the best protection from a law suit is a well written contract. The realities of business make such contracts very nearly a necessity.

4.5. Impact on Access and Privacy

As can be seen from the preceding sections, the gamut of institutional issues related to the use of information, particularly in a distributed environment, is very broad. The

breadth of the issues is only just beginning to be realized and it continues to expand as technology exposes us to quandaries that our law is not well equipped to handle. The active pursuit, and at least the embryonic forms of resolution, of these problems is necessary before the use of distributed information systems becomes widespread and commonplace.

Due to the complexity of the issues, there is bound to be some conflict between the right to privacy and the right to access. Discord may also be found in any of the influencing factors discussed. For instance, disagreement arises between the right to access government-held information at a cheap rate and the right of information holders to charge realistic prices for the use of their information. This issue revolves around the increasing realization of the commercial worth of information. It is recognized on the one hand that the widespread use of information, effected through ease of access and minimal cost impediment, is beneficial to the community at large. On the other hand, the creation and maintenance of information requires the expenditure of resources. A balance must be struck between public benefit and commercial reality.

Land information, while not likely to cause as much contention as personal information, must be used carefully to avoid unwarranted invasions of privacy. Information managers owe a duty of care, to both the information providers and the information users, to disseminate accurate information that is released only within the bounds of a secure environment. This environment must be established and maintained through the balanced use of technology and policy.

There is a large and ever growing dependence on computer technology in today's society. When compared to the level of dependence, the occurrence of computer error would seem to be tolerable. The potential, however, exists for large numbers of people to be wronged as the result of reliance on information that is later found to be in error [OECD, 1983]. In providing access to information, database owners must be mindful of the liability to which they are exposed.

Existing legislation is not totally applicable to information. At present, most legislation deals more with the medium through which information is communicated, or on which it is stored. The technology is regulated, not the information. In addition, existing legislation and policies do not recognize the problems of operating in an environment that uses computer programs, expert systems and distributed databases [Branscomb, 1988]. There is a need to explicitly recognize information as an entity unto itself, capable of being dealt with as an end in itself, rather than being some form of attribute attached to a more tangible physical object.

Increasingly sophisticated technology is creating increasingly complex problems. The speed with which technology is advancing is not being matched by the speed with which social values and formal legal solutions are advancing. There is a need to pro-actively pursue the solutions to some of the institutional problems associated with the use of information and to produce policies to act as guidelines for those who wish to use information.

Institutional matters are often considered to be the domain of the public sector, however, the initiative of the private sector is an important element. The cooperation of the public and private sectors is necessary if an effective distributed information environment is to be developed. There are skills in the private sector that are relatively scarce in the public sector. If the private sector is not forthcoming, however, there is the likelihood that information systems will be developed without their assistance, perhaps to the detriment of the final product.

Figure 3 depicts the interrelated nature of institutional issues. It illustrates the fact that it is difficult to discuss one topic without being aware of the interplay of the others. The web formed by the association of one element with the others is complex.

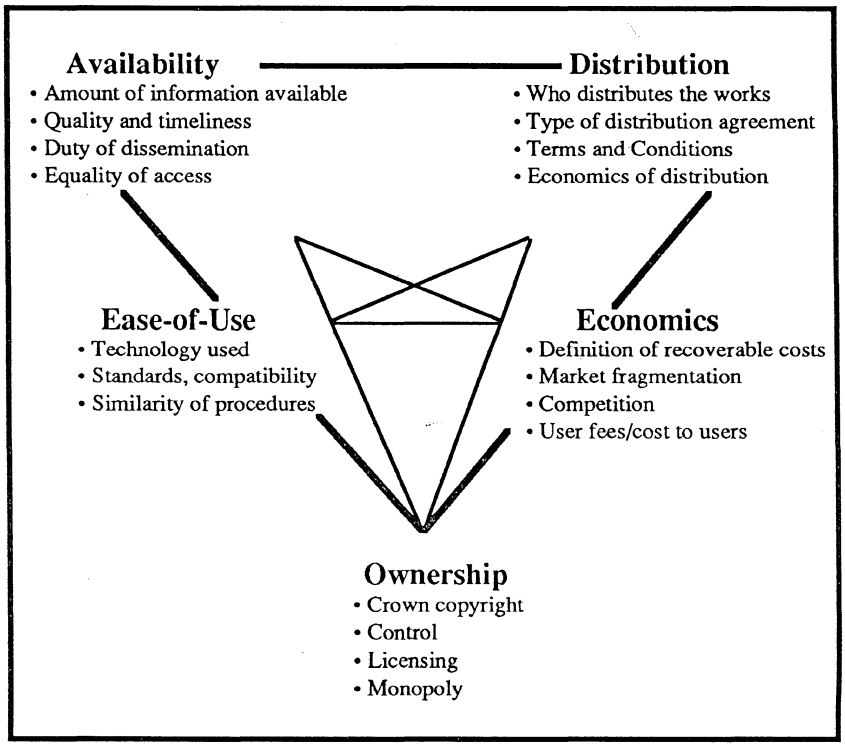


Fig. 3. Issues Related to Ownership (from CLIC [1991, p. 26])

4.5.1. Control of Information

Any custodian or owner of a database has an obligation to see that the data resource is properly managed. In the case of the public sector the public interest is of paramount importance. The public sector should be "guided by the presumption ... that open communication and the free flow of information have great social utility" [Shattuck and Spence, 1988]. The private sector is less motivated by the value of public interest, being more influenced by the demands of the market. Private sector products and services must satisfy a demand for the business to remain viable. In either case, good management requires control over the data resource [CLIC, 1991].

Privacy, by definition, requires a degree of control over information and its use. This control can range from a veto on its collection, to determining under what circumstances it may be released. Control over information is most commonly thought of in the privacy setting, yet it is no less important in the context of access. Control over the use of information is a necessary requirement, particularly in a commercial environment. Economics, data quality, liability, etc., cannot be effectively managed if control cannot be enforced.

4.5.1.1. Use of Copyright

Copyright is one of the most popular and presently the most appropriate means of exerting control over land related information. This is not to say that enforcement of copyright is easy, as can be attested by those battling against software piracy. Support for copyright over government-held data can be justified subject to at least two caveats [CLIC, 1991]:

- The rights granted to copyright holders must not be used to restrict access to public data.
- Government custodians must be cognizant of the fact that not all information within their keeping is available for distribution. This statement is made in light of the fact that one of the uses of copyright is to protect the right of economic gain from the sale of information. The use of copyright as an exclusive license to sell information is in all cases subservient to the need to be aware of the requirement to protect information privacy. The protection of information privacy can be effected through copyright, just as successfully as it is used to control the sale of information.

4.5.1.2. Use of Freedom of Information Legislation

Most access to information legislation requires government-held information to be made available at what can be described as dissemination costs only. This would seem to conflict with the commonly held view of the use of copyright. One of the purposes of copyright is to protect the copyrighted material so as to encourage innovation [Branscomb, 1988]. In a commercial sense it is difficult to encourage innovation if the effort that goes into it is not adequately rewarded.

The apparent conflict between copyright and freedom of information legislation is nonexistent in some cases, but has yet to be adequately resolved in others, as shown in the following examples:

- It is generally accepted that access to information legislation cannot be used to secure information that is already publicly available [Saskatchewan Freedom of Information and Protection of Privacy Act, 1991; Province of New Brunswick, 1990]. The Saskatchewan legislation clearly states in section 3(1) that the provisions of the Act do not apply to "published material or material that is available for purchase by the public". If government is making an active effort to provide information to the public, the public has no recourse to freedom of information legislation. It is only information that is not generally available that may be the subject of a disclosure request.
- Obtaining a copy of a database, or part of a database, via a request made under freedom of information legislation, does not entitle the recipient to reproduce, copy, sell or redistribute that data. This right must be obtained separately and explicitly from the database owner or custodian. In this sense the concept of ownership and rights of control over information are preserved through copyright. The holder of the copyright has the sole right to permit certain activities involving the use of the information.
- Access to data is in some cases only half the battle. If the data is to be of maximum benefit the software and algorithms that are used to manipulate the data must form an integral part of any information package received. In many instances it is likely that the very legislation which provides for disclosure of the information will also prevent provision of the necessary software. This situation will arise if the software has been provided by a third party vendor and is proprietary in nature. It is likely that the exemption found in most freedom of information legislation relating to non-disclosure of proprietary information will extend to include

proprietary software. In such a case the software could not be transferred to the requesting party. Even if the software is not considered to fall within the realm of proprietary information exempted by the legislation, the standard copyright protection of software would likely effectively curtail its transfer to the requesting party by government [Perritt, 1989a].

In opposition to the view that database management and retrieval software should not be included in any information package disclosed by government, is the opinion that such software is an integral part of the database and must be released. If the data and the software that comprise the database are not segregable, the status of the software under freedom of information legislation is questionable [Office of Technology Assessment, 1988]. In the U.S. it is argued that, barring any intellectual property interests held by an individual or company, given the spirit of freedom of information legislation, the public should be permitted access to the data in the software environment in which the data is maintained [Kahin, 1991].

4.5.2. Commercialization and Competition

One point of view relating to commercialization and competition is that government should not sell information, which it is mandated to collect and use, at anything more than dissemination costs. This approach provides all people with cheap access to the basic information resource used by government and paid for by tax dollars.

The availability of vast quantities of information at low prices eliminates one of the major impediments to the development of a private sector information industry. It will encourage private sector investment in information resources, products and services [Chartrand, 1987]. It is argued that in these early days of digital land related information such an approach is necessary due to lack of undisputed evidence regarding the size of the potential market [Epstein, 1992]. If overly optimistic assessments of the market are made, resulting in government attempting to recoup more than dissemination costs, the private sector information industry may be stifled before it has the chance to establish a firm base from which to expand.

There is a tendency to overestimate the market possibilities for information. It is important to note that "the vast majority of database vendors in the private sector are not earning robust profits because of high costs and other factors. The top 10 databases in the U.S. account for 80% of the market. Most databases lose money" [CLIC, 1991]. Database vending is a very low profit margin business. There is a requirement to supply

information to a sufficiently large audience in order to assure success. In providing information services, the same criterion applies.

Private information vendors are clearly in favour of a dissemination costs only approach for the sale of government information. There is, however, some scope for government involvement in more than just the wholesaling of information. Some examples of when retailing activities on the part of the public sector may be warranted include:

- If the private sector is not meeting the needs of the public, government has a role in filling the void, or providing an improved service;
- Some information is not attractive to the private sector, as the demand, and hence the profit earning capacity, for it is not high. For such information it is up to government to ensure that accessibility is maintained as a matter of public benefit;
- Government agencies could develop a commercial arm to satisfy the needs of certain users whose needs are not being met, or whose interests are not being served. The establishment of such a government retailer may not conflict with the role of government as a wholesaler if the base information used by government is still available to those who want it in its raw form at dissemination costs [Perritt, 1989b].

Interestingly, it can also be postulated that freedom of information and the concept of not charging for mandated information activities, can itself pose a threat to private entrepreneurs [Perritt, 1990]. The fear is that systems may be developed that manufacture significant added value in order to aid government in fulfilling its mandate. Adhering to the argument that information required for mandated activities should be available at dissemination costs, there is the possibility that significantly value-added information would be available at relatively low cost. If this should occur it will be difficult for private sector entrepreneurs to recover investments made in adding value to public information themselves.

5. Security

Security may be defined as the protection of information from unauthorized or accidental modification, destruction, disclosure and use (or denial of use) [Jackson, 1990]. As an aid to determining whether established security measures are adequate, the information qualities of integrity, availability and confidentiality must be monitored [Halliden, 1990]. It must be realized, however, that absolute protection is not possible and security is better understood as a form of risk management. Controls are implemented to reduce the probability and consequences of a security breach only to the extent that their cost is less than the damage likely to be incurred.

Over the years the focus of security has changed dramatically. In the 1950s and 60s the security of information was not perceived as a critical issue. In that era the resource of greatest value was not information, but the computer itself. Physical security of the computer plant was the prime concern.

In the 1970s an increasing number of organizations began to realize the benefits to be gained by utilizing computers. The use of computers lead to improved productivity, in part due to relatively fast access to large amounts of data. As a result, the focus of security shifted from the physical control of the computer to the control of data. In this period, data security needs were met by such responses as simple password control measures and increasing attention to physical security in the form of fire suppression systems, offsite storage of data and software, and disaster recovery planning.

The 1980s saw the widespread introduction of low cost computing power and communication technology. Increasing dependence upon information with qualities such as timeliness and accuracy, and a spiralling reliance on technological tools that utilize information to provide decision support, led to a shift in the focus of security once again. Decisions made and actions taken based on the output of computers linked in amorphous distributed networks mandate that information security now assume prime importance [Jackson, 1990].

The acceptance of the importance of information security has increased over the last decade due to several factors:

- an increasing awareness of the value of information as an asset or resource which, depending on how it is managed or controlled, may have a significant bearing on the future of an organization;

- the threat of loss or damage to an organization should the information which it collects, stores, processes, or is otherwise responsible for, is compromised in some way;
- a realization that an investment in information security can be justified on a strictly commercial basis.

The commercial value of information security is often stressed, but privacy also relies heavily on effective security measures. In a distributed computing environment the availability of vast stores of data, and the computing resources to process that data, raise concerns related to privacy. The requirements set by the definition of privacy can in fact be met by security. Properly implemented, security can greatly enhance the ability to control:

- how information is collected;
- what information is collected;
- how information is used;
- by whom information is used [Jackson, 1990].

The establishment and growth of distributed networks increases the importance of coming to terms with security. When dealing with information, security is a function of hardware and software, database structure, the communication network and administrative procedures [Roitman, 1988]. When the term security is used, it can be applied in at least two ways:

- system security;
- data security.

It would seem that if system security measures are good enough then there is no need to be concerned with data security, as the data can only be accessed through the system. No system, however, is perfect, so there is a need to explicitly address data security, rather than assuming that it will be attended to by system security. To meet the security needs of a distributed environment comprehensively a two pronged approach is required. The two planes that must be addressed are:

- technology – issues such as identification, authentication, authorization, secure communications and auditing fall within the gamut of technical aids to security;
- policy – there is a need to identify the items of value and the vulnerability to which these objects are exposed.

5.1. Attributes of Security

In the past, security has often been thought of only in terms of access control. Now, however, it is more correctly associated with a system providing services which attempt to implement the risk management criteria set by data managers [Halliden, 1990]. The services provided typically act to preserve the confidentiality, integrity and availability of data to the desired degree. Parker [1991] discusses what each of these terms entails.

5.1.1. Confidentiality

Confidentiality is the state of being secret or known only to a select few. In a distributed computing environment confidentiality attempts to ensure that specified information is available only to those parties who have a need to know about it and have authorized access. Unauthorized disclosure of information is the prime example of violation of confidentiality.

When operating in a hostile environment the attribute of confidentiality may be extremely important. Likewise, from a privacy point of view, the notion of confidentiality must receive an adequate weight in the design of security measures. In a business environment, however, in which a degree of trust exists between all parties, profit, productivity and growth may be more important than confidentiality.

In a business environment in which a degree of correctly motivated cooperation exists, the interests of all parties may be best served by providing access to all information, unless otherwise stated. In a democracy also, the norm for data collected by government must be open access. This scenario, in which only a small amount of information is held as confidential is a reversal of the 'need-to-know' approach commonly adopted when confidentiality is considered.

5.1.2. Integrity

Integrity refers to the qualities of wholeness and completeness that exist in data. It is "the state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction" [Department of Defense, 1985]. Integrity relates to all information being present and accounted for. This is not to say that it is necessarily accurate or correct. Integrity deals with the degree of confidence that a user can have that the information received is identical to the source information.

The value of integrity is of greatest importance when data communication occurs. A high degree of information integrity will result in information reaching a remote user in a state of wholeness and unimpaired condition. No parts of the information are missing, concatenated, encrypted or converted in unanticipated ways.

5.1.3. Availability

Availability attempts to ensure that data and other resources are at all times accessible to authorized users. It refers to the ability to guarantee the presence of data. It does not necessarily mean that the data available is correct or usable.

In a distributed computing environment, availability is of great importance. Unfortunately, it is rarely included in formal security policies and is said to be the most ignored purpose of security with the exceptions of recovery planning and backup. In fact, data backup, redundancy planning and protection from physical harm are the principle means of implementing availability measures.

5.1.4. Utility and Authenticity

The above three attributes are those most commonly associated with security services. Parker [1991] contends that two additional attributes, utility and authenticity, are necessary if the service provided by the security system is to meet the needs of users.

Utility is the state of being useful for some specified purpose. For example, if information is in encrypted form and the end user does not have the ability to decode the message, the availability and confidentiality of the information may well be present, but the utility is nil.

Authenticity of information refers to the state of correctness and accuracy of representation. Whereas integrity preserves the intrinsic form of the information, authenticity preserves the extrinsic state of conformity to fact. Authenticity is typically used to validate the data source as being the one claimed. This attribute of security control is utilized when user passwords are checked.

Utility and authenticity are added to the list of confidentiality, integrity and availability due to the non-overlapping nature of all of the attributes. Without the two additional attributes the quality of information reaching a user may be inadequate.

5.1.5. Priority of Attributes

Parker [1991] states that if the above five attributes were listed in order of decreasing attention received, the list would read as follows: confidentiality, availability, authenticity, integrity, utility.

Confidentiality rates highest due to the efforts of civil rights advocates to increase our awareness of privacy principles, and also due to the efforts of governments keen to impress upon citizens the sensitive nature of some of the information for which it is responsible. Authenticity, integrity and utility are relegated to the bottom of the list as they are often regarded as mundane security practices which can be achieved through the use of routinely provided standard services.

Parker [1991] is of the opinion that a more appropriate ranking of these attributes would be as follows: availability, authenticity, integrity, utility, confidentiality. This order suits land related information particularly well, but it can be argued that it is also valid for all other information, including that of a personal nature.

The justification for placing greatest emphasis on availability is that if information is unavailable, all other security controls are irrelevant. No security problem can possibly exist if no one has access to the desired information. In a distributed environment this is a particularly salient point.

5.2. Technical Network Security

A computer network must have in place certain security measures to protect its resources from undesirable actions. A well balanced security programme must make use of both technical and non-technical solutions. It is unlikely that physical security measures by themselves will adequately meet the challenges of information security, but they do offer a good first line of defense [Jackson, 1990].

Technical security measures must specifically answer the following questions:

- What are the objects to which access must be controlled?
- What are the subjects whose access must be controlled?
- What are the threats which access controls must prevent?
- What are the mechanisms to enforce access controls? [Janson and Molva, 1991]

The first question refers to information, applications, network components and other resources available to users. The second question addresses who is to have access to the

system. The first two questions can be grouped together and paraphrased as 'what to protect from whom'. The third and fourth questions can likewise be grouped together and paraphrased as 'what to protect against and how to do it'.

5.2.1. Special Nature of Distributed Environments

Providing security services for a distributed computing environment is entirely different from securing a standalone system. Networks provide many data access paths, which are difficult to protect and greatly decrease the ability to effectively prevent intrusion [Rymer, 1990]. The requirements for information security (i.e., protection of integrity, availability, confidentiality, etc.) remain the same for distributed systems as for centralized systems, but the means of ensuring these controls is significantly altered [Jackson, 1990].

A distributed environment, being a collection of individual nodes connected via a communication network requires a security strategy that recognizes the issues associated with each of these two elements. The strategy developed must address the security needs of the individual nodes and the security requirements of the communication links between the nodes. The strategies developed for each of the components must be complementary in nature if they are to be effective. The overriding constraint is that no single authority is able to control the entire environment. The success of any security controls ultimately depend upon how diligently they are implemented by the authorities at each node [Rymer, 1990].

Security at the nodes is usually effected by use of standard techniques such as passwords and access control lists. This is no different from the controls that occur in a centralized system. The aim is to specify which resources on the system are available to which users and to provide mechanisms to prevent those who are not authorized from performing certain activities.

In a distributed environment, the danger of relying too heavily on standalone security mechanisms is that once an unauthorized party breaches the security shield, free access to the entire system is gained. For this reason, securing communications has become the focal point of distributed system security. Communications security seeks to protect the links between nodes on the network. Measures taken include checking user identities and privileges, encrypting data when necessary, and recording activities within the environment. All of these activities must be carried out in an integrated, system wide manner.

5.2.2. Identity

In a distributed environment it is possible that every user will have a different authorization level for the information resources contained within the system. It is also possible that there will be no correlation between individual authorization status and the system at which that individual is physically located. Therefore it is necessary that some form of user identification, usually in the form of a username, be employed that is capable of uniquely identifying an individual. Particularly when access to remote systems occurs, it is necessary for the remote system to know exactly who it is dealing with, not just the identity of the system on which the user is located [Rymer, 1990].

The user's identity is necessary to determine what functions that individual is permitted to perform. Access control policies depend on being able to determine the identity of individual users to allocate user privileges.

5.2.3. Authentication

Once a user's identity has been established it is then necessary to verify or authenticate that users are who they say they are. The user must offer some proof of identity. Secret passwords are the typical means of implementing authentication.

Although passwords are the standard means of authentication, there are three generally recognized means of providing this security control. The individual may be required to offer one of these three, or a combination of them, depending on the approach adopted by the security administrator at each system:

- Identifying possession – this usually takes the form of a plastic magnetically encoded card. Other varieties of card type technology may be used to provide authentication.
- Identifying knowledge – the generally adopted secret password is an example of knowledge that an individual must possess in order to authenticate identity. In a distributed environment it is necessary that every password be available to every system connected to the network to enable the authentication process to be carried out. This in itself can create a security problem. Many password authentication mechanisms rely heavily on encryption to help alleviate this problem. While this method undoubtedly ensures the security of passwords, it does incur system overhead costs.
- Identifying physical characteristics – this means of authentication utilizes so called unforgeable identifiers, or biometrics [Janson and Molva, 1991]. Examples of

these include finger prints, voice recognition and iris scans. These techniques are likely to provide the most reliable and robust means of authentication in the future, however, at present they are generally expensive and as yet have not been perfected. While it is not likely that an unauthorized user could masquerade as an authorized user, it is possible that the security mechanism will not recognize the genuine user from time to time due to the immature nature of the technology.

5.2.4. Authorization

Once identity has been established and authenticated there is a need to determine what resources and services are at the disposal of the user. Access control lists are a common basis for distributed authorization services. Access control lists specify what resources are available to whom, and what those authorized users may do with the resources.

There are typically three levels of access control:

1. confidentiality or secrecy controls – mechanisms that protect resources (data, media, input devices) from being generically read by unauthorized users;
2. integrity controls – mechanisms that protect resources (data, media, output devices) from being generically written (appended to, modified, erased, deleted, or otherwise affected in state or content) by unauthorized users;
3. availability controls – mechanisms that protect resources (programs, processors, memory channels, devices, buffers, routes, tables, etc.) from being used by unauthorized parties, especially if it would curtail or even deny their usability by legitimate users [Janson and Molva, 1991].

Authorization controls are valuable security tools that can be used to reduce the chances of system resources being compromised as a result of human error, accidents or omissions. They can also help protect against deliberate acts of sabotage by dishonest or disgruntled employees. Particularly relevant to a distributed system, is that they are also beneficial in reducing the likelihood of excessive damage resulting from system penetration by outsiders. The actions of unauthorized intruders will be limited to those that are available to the user who they masquerade as to gain access to the system.

5.2.5. Secure Communications

Encryption is the means by which maximum communication security can be obtained. It involves processing communications through a mathematical algorithm which scrambles

transmissions into unintelligible streams of data. Encryption is an excellent tool when highly confidential or sensitive information is to be transmitted across a network.

The concept of encryption requires the communicating parties to agree on the scheme to code and decode information. Messages are encoded and decoded using unique numerical keys. These keys may be secret or, as with the public key encryption system, comprised of a public key and a private key used in conjunction. Having encrypted the information, it may travel securely over the network to its destination. Even if the information is intercepted, it is unlikely that the interceptor would be able to make any use of the encrypted information [Schweitzer, 1990].

Cryptography has several roles to play in communication security:

- secure authentication and authorization services;
- protect communication channels;
- secure actual messages travelling across the network;
- detect modification in messages or transactions [Rymer, 1990].

The main concern about encryption is that it incurs a high system overhead cost (in the order of 10 – 15% [Rymer, 1990]). Bearing in mind that security should only be implemented at a cost that is less than any anticipated potential losses, encryption should only be used for the most sensitive of information. Some form of cost benefit analysis is warranted to justify the use of this tool.

5.2.6. Auditing

The audit function is used to enforce accountability on users and to aid in after-the-fact investigation of security breaches. Auditing can be a somewhat complex administrative procedure, and apart from the difficulty of coordinating such an activity over a distributed environment, it can also add up to 10 – 12 % to system overhead costs [Rymer, 1990]. Authentication and authorization information must be recorded in addition to what exactly was done to which data.

5.3. Levels of Security

Security systems in general provide multiple levels or layers of security. Each layer serves to detect, discourage or deter an unauthorized user or intruder in its own manner, with the set of features with which it is endowed. Any layer taken on its own may not be sufficient to prevent the infiltration of the system, but the combination of the security

measures should provide for protection to the extent that the system administrators feel is warranted for the value of the information held. The security layers typically referred to and relied upon are listed below [Schweitzer, 1990; Dale and McLaughlin, 1988]:

- Legal framework – this is the laws and regulations that exist to deal with broad social issues in the environment in which the system is situated. To discourage or respond to breaches of computer security, laws relating to security and privacy may be employed. If the laws do not serve as an effective deterrent, and more technical and physical measures are not sufficiently effective as preventative measures, then the law is seen as the final recourse to punish intruders after-the-act. As has been stated previously, the law is not well suited to deal with crimes involving information, although this situation is slowly changing.

- Physical security – this is the means by which an attempt is made to prevent unauthorized parties from coming in physical contact in any way with the computing environment or the computer resources. Physical protection can take the form of guards, receptionists, door access controls such as keys, combination locks, magnetic cards, etc., restricted access areas, fencing, etc. These measures attempt to keep unauthorized parties out of the physical spaces in which computer resources are located.

  In a distributed computing environment, physical security may be difficult to maintain and is likely to be ineffectual, and possibly irrelevant, in any case. Access to the system is more likely to come through illegal entry to the network from a remote terminal than illegal physical entry.

- Administrative and procedural controls – these controls are provided mainly in an attempt to lessen the likelihood of an 'insider' performing unauthorized activities. According to Jackson [1990], 70 – 80% of all security threats come from insiders. These controls strive to protect the integrity of the data assets from accidental or malicious damage.

  These controls may be implemented by:

  – authorization schemes in which the access and use of resources are specified for individual users;

  – use of independent or neutral parties to provide objective checks and balances on activities (i.e., separation of powers);

  – regular activities designed to provide quality assurance functions over the resources;

– auditing of activity;

– use of intellectual property ownership agreements and other contractual arrangements to control the environment.

- Logical security – this layer of security is provided by hardware and/or software features that are usually provided by the system. This layer of security typically takes the form of password control, authentication and authorization (i.e., access management capabilities).
- Data transformation – This refers to the encryption of information and will likely only be used for information of a highly sensitive or confidential nature. User password keys may use this level of security. There may be some organizations that do not require data transformation at all due to the non-likelihood of unauthorized entry or the value of the information not being worth the expense of protecting it to such an extent.

Figure 4 shows one possible scenario for security control using the elements listed above. The number of layers actually employed, their order, and the possible merger of two or more layers will depend upon such factors as:

- the needs and resources of the organization;
- the internal structure of the organization;
- the external environment in which the organization operates;
- the perceived threat of invasion;
- the value of the resources available through the system.

The view taken as to what measures are necessary and in what order to implement them may also depend on how an organization views the security function. For instance, an organization which is used to operating in a standalone capacity is more likely to require security to prevent unauthorized intrusion into their node. Other organizations, which are more comfortable with the distributed concept and with outsiders having access to their resources, may desire the security mechanisms to act more as a resource control mechanism rather than an outright access prevention mechanism.

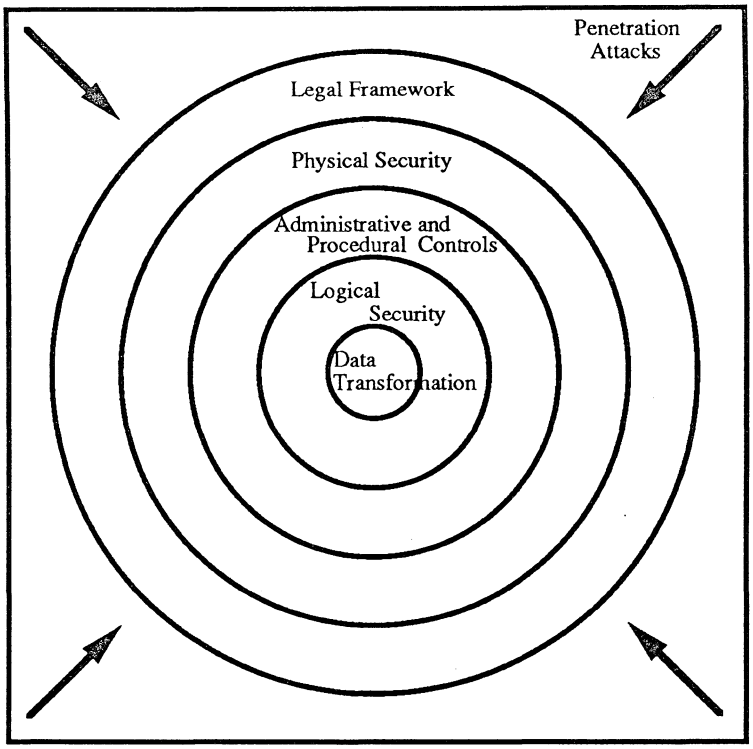


Fig. 4. Concentric Levels of Protection (after Schweitzer [1990, p. 71])

Taking this example further, the first organization may see legal controls as a means of prosecuting intruders, whereas the second organization may wish to utilize legal controls to establish contracts and data use agreements. In this case, the positioning of legal controls may vary in the concentric ring model of security layers. As has been demonstrated, each security layer can be used in a reactive or proactive manner.

5.4. Information Classification for Access Control

Information access control is concerned with ensuring that users and processes in a distributed computing environment access information in a controlled and authorized manner [Moffett et al., 1990]. For any policy regarding access control to have a successful outcome it must, at a minimum, attempt to implement the following three process:

- determine the value (both tangible and intangible) of information and classify it accordingly so as to indicate the appropriate information management response required;
- establish authorization requirements for users and instruct information custodians on how the authorization process is to take place;

- periodically review the authorization process and redress any weaknesses that may be apparent [Jackson, 1990].

The aim of access control is to govern the information environment. The expected outcomes of this governance include a decline in the misuse of information, and the maintenance or enhancement of the quality of the information resource. Access control is clearly an important component in security measures. Classification of information, a mandatory access control activity, is therefore an element essential for the handling of information.

Two extremes of access control exist:

- Open access – an environment in which the default level of security for all information is set to open access. The small percentage of information that requires stricter access controls will have its security level upgraded on a case-by-case basis. Access to information legislation adopts this approach as a model. The public is permitted to access all information except that which is specifically exempted from disclosure. This approach suits land related information well, as the bulk of such information is already a matter of public record and is therefore not likely to become embroiled in controversy relating to privacy. This openness will likely lead to an increased ease of accessibility which in turn may increase the security risks incurred.
- Restricted access – an environment in which the default setting for all information is that of confidential. Information desired for general access must have its security classification altered. Information availability in a system in which access controls are oriented towards restriction may ultimately reach the same state of access equilibrium as would occur in a system biased towards openness, but the system will err on the side of caution by creating an initial state of confidentiality for all information. Systems which contain large amounts of personal data may prefer to adopt this option.

Whether one of these extremes is chosen, or an option that takes some middle ground, to all information there must be attached some objective rules which apply to those who wish to access the information. These rules will likely have been formulated in response to factors such as those listed below:

- The circumstances under which the information was acquired. Information may have been supplied voluntarily and without thought of any form of compensation, in exchange for some perceived benefit, or under the compulsion of law. Each of

these circumstances, and any others that may arise, will dictate to a certain extent the rights that an individual has to information access.

- The type of information being released. The information released should not violate a person's privacy or offer unfair commercial advantages. A minimum requirement of the information being released is that it be accurate and not misleading.
- The persons to whom the information is being released and the purposes for which the information is being acquired. When initial collection occurs, the party supplying the data should be made aware of the uses to which the information will be put. Their free and informed consent (implied or explicit) for the use of the information should be sought.
- The ability to control the uses to which the release of information will be put after it has been released. This is perhaps the most difficult issue to deal with. Although copyright and contracts may be used to try to control the use of information, they rely to a large extent on the honesty of the end user. It is also possible that some uses not in breach of any legal agreement, but undesirable none the less, will be made of information.
- The effect of release of information on public support for increased accessibility of information. Any misuse of information is objectionable and may make it difficult to gain and maintain the confidence of the public. Despite the benefits that may be available through the analysis and integration of data sets, if frequent and sufficiently harmful abuses occur, the public will be intimidated and their support for improved accessibility will likely wane [Cuming, 1991].

The classification of information is one means by which a framework can be created to apply some objectivity to the issue of access control. Objectivity may be increased by identifying the vulnerability of information, establishing guidelines for determining if correct classification has taken place, and being cognizant of the degree of management required and the results that protection is likely to achieve.

5.4.1. Information Vulnerability

Information vulnerability may occur in a variety of forms. Loss or exposure of information may be brought about intentionally or unintentionally, by trusted parties or unauthorized adversaries, or by parties within or external to an organization. Each of these variables must be taken into account when the following categories of information vulnerability are considered [Schweitzer, 1990]:

- Exposure – unauthorized observation of information. Exposure of information may occur without the owner being aware that it has happened. The information is not necessarily removed from the system or destroyed, but becomes knowledge of parties who are not intended to know about the content.
- Destruction – can occur as the result of a natural disaster, such as fire or flood; by carelessness on the part of insiders in preparation, handling or processing of information; or by deliberate acts of revenge or aggression. Destruction of information is harmful, but at least such actions are blatant. More dangerous are subtle changes to information that may occur from modification, or a decrease in the value of the information as a result of exposure. Disaster recovery planning should effectively minimize any damage and inconvenience caused by destruction.
- Denial of access – the information contained within the system may be safely in tact, but due to some break in the communication network, or other reason, it is not able to be accessed. Such circumstances may be brought about by deliberate acts of sabotage or accidents such as fire and flooding. Physical threats such as fire and flooding account for 20 – 25% of threats to information system security [Jackson, 1990]. This issue highlights the importance of access, especially for a distributed environment. Even if the data is present, if it is not able to be utilized its existence is of no value.
- Theft – the unauthorized removal of resources takes an interesting twist when dealing with information. The theft of information often involves the copying or observation of information rather than the removal of the asset as is commonly associated with the concept of theft. The original information may be left in its place and the owner is not denied the use of that information. The result of the theft may be a decrease in the value of the information to the original owner, which is similar in concept to theft of more traditional assets.
- Unauthorized change or modification – may be very difficult to detect. Physical access to the data is not required to effect the change and humans are not inherently capable of detecting the state of information in their custodianship. It is often not until an attempt to use the information occurs that flaws such as loss of integrity and utility, brought about by the modification, are detected.

5.4.2. Classification of Information

It is generally too expensive to provide high level protection to all information contained within a system. Information must be protected at a level commensurate with its value.

The value of information will vary depending upon the criteria by which it is judged. The correct classification of information will have a direct impact on the success of the security system. Incorrect classification may result in a poor investment of security resources, or worse, the misuse of sensitive information.

Privacy is seen by many as one of the main criterion by which information should be classified. The difficulty in defining privacy, alluded to previously, is reflected in the difficulty of protecting privacy itself. Wacks [1989] suggests that greater success may be had by identifying what specific interests of an individual ought to be protected, i.e., personal, sensitive information. Westin [1967] states

> The first way we can try to come to grips with [the problem of loss of privacy] is to develop a new way of classifying information, to identify what is private and 'non-circulating'; what is confidential, with limited circulation; and what is public or freely circulating. This can also be seen as a distinction between the facts about ourselves that are intimate; those that are part of our life transactions (education, employment, family, etc.), and those that are formal public records.

Other criteria may also be used to create a classification hierarchy. For instance, the sensitivity and confidentiality of information in a business environment might depend on its affect on the financial performance of the organization, or the degree to which it enables effective and efficient work to be carried out. Schweitzer [1990] suggests that however the classification types are derived, two or three are all that are required and manageable.

Schweitzer [1990] and Jackson [1990] both provide examples of information classification levels appropriate in a business setting:

- Highest classification – confidential, registered or restricted information. This information is highly confidential and/or sensitive and must be tightly controlled and accounted for. Unauthorized disclosure of information with this classification level may result in serious damage to the organization. Information at this level may warrant encryption when transmitted over the network.
- Middle classification – private or business only information. This information, if improperly disclosed or used, would not be in the best interests of the organization or its customers or employees.
- Lowest classification – general or internal use information. This information does not require any protection against disclosure within the organization. This

information is still the property of the organization and discretion may be required to prevent its improper use from causing embarrassment.

There is of course one remaining classification, that being unclassified. Information falling within this grouping may be general knowledge and other information over which no proprietary claim can be made.

Schweitzer postulates that only 10% of all business information need be classified, and that less than 1% of information requires the highest level of classification. For land related information, much of which has been collected by government, Schweitzer's approximation should serve as a worst case scenario. If the full benefits of a distributed environment are to be realized there is a necessity for open access. Rather than adopting a need-to-know approach, in which only those with a special need to access certain information are given authorization, a need-to-restrict approach may be more appropriate. This approach makes all information available to all people unless there are extenuating circumstances, in which case the authorization for certain people to perform certain actions on certain information is withdrawn.

Based on the classification model given above, the following is an example of a classification system which may be appropriate for government land related information:

- Confidential – this information has been gathered by government to enable it to carry out its mandated function. This information is generally of a private and proprietary nature and specifically identifies individual people. It is not to be released for general access unless explicit permission has been granted by the information owner. An invasion of privacy would occur if this information were disclosed.
- Sensitive – this category may include information which although collected and used by government is not part of the public record and is not to be distributed to the public as a matter of course. Having collected the information, the government may have been granted explicit or implied permission to use the information as it sees fit. It may be used widely within government and may even be made available to members of the general public upon their request (perhaps subsequent to some aggregation, depersonalization, or desensitization).
- General or public record – this is information that forms part of the public record or can be observed by anyone with a minimum of effort. It does not contain information that are regarded as private facts. This public information can be regarded as belonging to the people, but is held in trust by government and made

available for open and uninhibited access [National Commission on Libraries and Information Science, 1990]. General information is not particularly sensitive and people are willing to offer it in return for the advantages that its collection and storage confer. Although not sensitive, a certain degree of discretion and care must be exercised to avoid it being misused, i.e., used for purposes for which it was never intended and which may be harmful, used in circumstances which yield misleading results, etc. This category will hold the vast majority of all land related information.

The information falling within each class is critically dependant upon the classification definition. In turn, the rules associated with the control of information are directly related to the classification level of information. Hence, the classification definition has an important bearing on the access rules which apply to a given set of information. An example of this is found in the Ontario Municipal Freedom of Information and Protection of Privacy Act, 1989. Section 2 of this legislation defines a personal information bank as "a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual." It is the assessment of Wilkinson [1991] that following from this definition, if personal information is collected and stored in a database, but its retrieval cannot be effected by searching on such fields as name or identifying number, then this database is no longer included in the definition of a personal data bank. By eluding the 'personal data' classification a host of restrictions connected with this class of information are avoided. At this stage it must be stressed that security should not be viewed as a source of irritation or something to be circumvented. It performs the important task of protecting the individuals and organizations with which information is associated.

5.4.3. Determining Correct Classification

Correct classification of information will be a determining factor in the efficiency of security controls. There is a need for people to understand the purpose for classification and to have a clear set of guidelines to help make the correct classification decisions. Ultimately, however, suitable classification relies on experience and good judgement [Schweitzer, 1990].

Schweitzer states that a set of classification indicators are needed to guide classification decisions. An example of these indicators is:

1. How many people are authorized to have this information?

2. How valuable is this information?
3. How sensitive is this information?

Questions may be asked of information in the context of each of these indicators. Depending on the answer, the information will be classified at a high, medium or low security level for each indicator. The sum of these results will point to the level of security appropriate for the information in question.

Parker [1989] provides a slightly different approach to determining the level of security of information. This approach is appropriate for business information and is used specifically to determine at what stage disclosure may occur. It intrinsically poses the three questions stated above by Schweitzer. From it the classification of information can be inferred. If information is not disclosed at a particular step, the user should proceed to the subsequent step.

- If the information is already public knowledge it may be disclosed. If, however, the information is generally known but disclosure of the source may expose a vulnerability it should not be disseminated from an identifiable source. In a strictly commercial environment if further disclosure provides no useful benefit to the discloser there is little justification for involvement.
- Information may be disclosed to anyone with an authorized need-to-know and if it does not aid an adversary.
- Disclosure is acceptable if it results in a net benefit. In determining the net benefit it is necessary to assess the value of all exchanges. This may be an extremely difficult process.
- If the information can be disclosed without identifying the source or resulting in any harm to the source, disclosure may proceed.
- If authorization for disclosure can be obtained from a higher authority (i.e., management) disclosure may occur.

The above list is extremely pragmatic and business-like. It may be difficult to apply such a classification guide to information of the type for which the public sector is responsible. Typically government-held information has a large public good factor included in its value. If this factor can be calculated accurately, the above system may prove to be workable, but evaluating intangible benefits and the protection of such concepts as privacy and open access to public information is notoriously difficult.

Without correct classification decisions, or some other means of arriving at appropriate security measures, it may prove difficult to be sure of the quality of information available throughout the distributed environment.

5.4.4. Protecting and Managing Information

Information classification is but one of the tools that may be used to establish what level of protection to offer information resources. It enables the critical qualities of information to be identified and the appropriate security controls to then be applied. Ideally the security controls employed will:

- be commensurate with the value of the information;
- incur a low, or at least acceptable, administrative overhead;
- not interfere unduly with the usual use of information;
- be automatically enforceable to a large extent.

Access control software is used to meet a number of these requirements. It acts to limit user access to information and system resources and also provides various audit functions. Access control lists are a major component of such software.

Access control lists are in essence a matrix which specifies or authorizes the interactions between users, data and processes [Moffett et al., 1990]. Figure 5 illustrates the matrix concept. The access control list or matrix works well in situations where the number of users is not overwhelming, however, Moffett et al. content that the standard access matrix is unsuitable for large distributed systems. The reasons for this inadequacy include:

- It becomes too large when the number of objects can be in the hundreds of thousands. Sparse matrix storage mechanisms can alleviate the problem to some extent, but it is necessary to partition the matrix. Domains provide a possible method of partitioning.
- The matrix, as a centralized data structure, assumes global knowledge of the user and target objects which are in the system, but it is impractical to maintain this global information in a distributed system spanning multiple independent organizations, so the full matrix can never be constructed.
- The access matrix is based on the assumption that access rights are specified between individual users and target objects. It does not permit policy to be specified with respect to groups, i.e. to domains. The manager may not even know the members of the domain at the time the policy is formulated, and the policy specification should not require changes when the individual user and target objects in the system change.

- We require a means of specifying policy in terms of roles performed by users in an organization rather than the users themselves. For example, the access rights for a departmental manager should not relate to the person holding that position, but rather to the position or role itself. This means the rights do not have to be changed if the person is moved to another role.

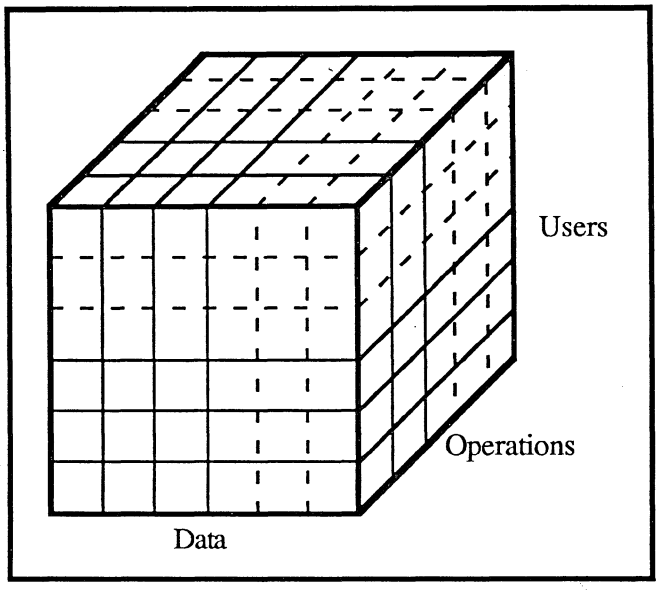


Fig. 5. Access Control Matrix

Moffett et al. suggest the use of domains and access rules may provide a more suitable means of controlling access in a distributed environment. Domains are collections of objects to which a common management policy applies. Objects refer to collections of users and collections of data elements. By grouping individual elements into domains, a flexible and pragmatic means is provided of specifying boundaries of management responsibility and authority.

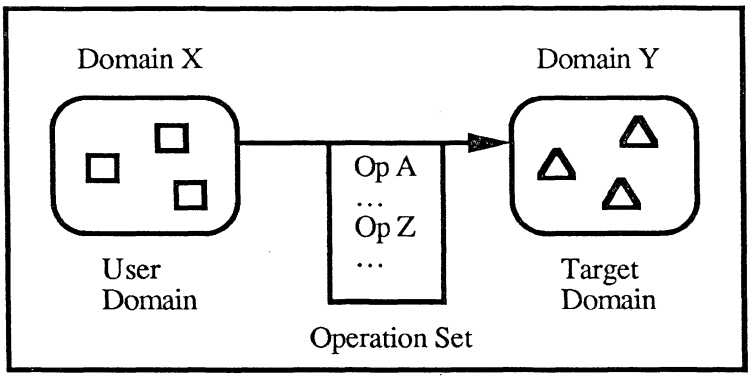


Fig. 6. An Access Rule (from Moffett et al. [1990, p. 573])

The access rules which operate on the domains are used to specify:

- the user domain – the set of possible users with the same or similar requirements for data and processes;
- the target domain – the data that may be operated upon;
- the operation set – the authorized operations that a user may perform on a target.

Whatever the means of implementation, the control of the data resource must be carried out in a manner that satisfies the needs of users. The protection of information, however, is only one of the facets of information security. Privacy, access and realization of commercial value, among other issues, must all be handled, to some degree, by the security function. Hence, it can be seen that security is an integral component required for the comprehensive management of information resources.

Information management refers to responsibilities for:

> • Optimizing benefits and minimizing overall costs to the business for providing useful information as needed to make good decisions and to increase profits.
>
> • Organizing information elements used in the business to give optimal support to the above.
>
> • Providing technology applications so that the business will realize benefits from its information, beyond mere need-to-know data, in a timely and efficient manner [Schweitzer, 1990].

5.5. Balanced Use of Security

The establishment and maintenance of a secure computing environment is a difficult goal to achieve. One of the hardest parts of this task is to strike the right balance between a

system that is user friendly and flexible while still retaining control of valuable resources. Balancing the use of security can be taken in at least two contexts:

- the cost of security measures against the threat of potential loss;
- the best mix of policy solutions and technical solutions.

5.5.1. The Cost of Security

A recurring theme in the literature is that absolute security is neither possible nor desirable [Johnson, 1991; Halliden, 1990; Rymer, 1990; Jackson, 1990]. At first it may seem that too much security can never be enough. All security, however, exacts a price in terms of inconvenience and cost.

Rymer [1990] contends that it is impossible to eliminate all of the risks to security. In addition "most commercial undertakings are not interested in perfect security" [Halliden, 1990] and are content instead to accept a degree of insecurity as a risk of doing business. The need for absolute security must be balanced against the need to provide an environment in which restrictions are not so great as to prevent or retard the effective performance of users' authorized activities. Absolute security may not be possible, but what may be more important is that users know what security is provided and have absolute confidence that the system will adequately carry out the security functions it is designed to perform.

The cost of providing security and the cost incurred if losses occur as the result of lack of security are the two sides of the equation that must be balanced. There are of course some indirect elements associated with both sides of the equation:

- security breaches cause loss of customer confidence, loss of staff morale, encourage further breaches, etc.;
- security controls reduce individual flexibility, involve management overhead, etc [Halliden, 1990].

To establish the correct balance it is necessary to be cognizant of the environment in which the system operates. An understanding of the degrees of success that can be achieved by the planned security controls is also important.

The penetration work factor (PWF) refers to the effort that an intruder must exert in order to reach his or her desired objective. For any organization, "security is established with the goal of extending the PWF to the point at which the perceived value of the target (information or mischief) is less than the perceived value of the penetration effort"

Schweitzer, 1990]. Figure 7 illustrates the point that a compromise exists between protection from unauthorized intrusion and ease of access.

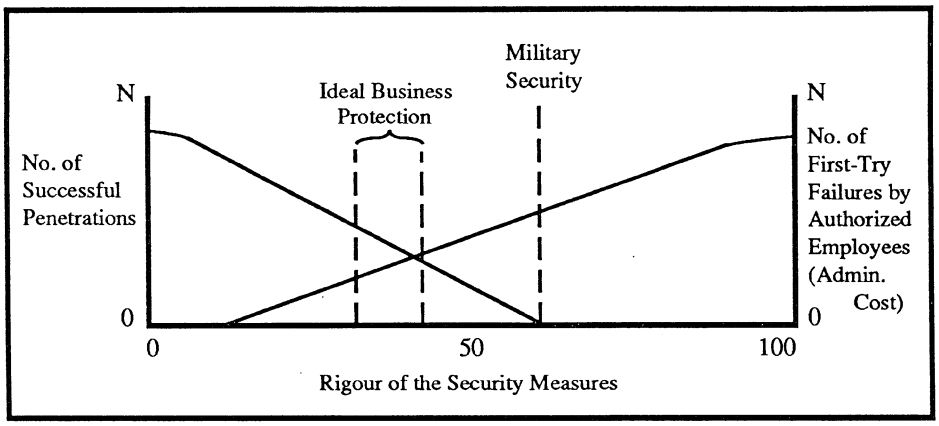


Fig. 7. Penetration Work Factor Versus Cost (from Schweitzer [1990, p. 122])

The appropriate level of security will vary from organization to organization, and may also vary within each organization. For some applications elaborate security will be required while in other cases security will not be a significant concern. It all depends upon the circumstances in question. To satisfy such variable conditions, it is necessary that the security controls be flexible enough to be set appropriately for a given set of users and a given set of circumstances.

5.5.2. Policy and Technology

> Protecting information security and integrity requires a combination of technical and non-technical approaches to be successful. Information security administrators should expect to devote approximately one third of their time to addressing technical aspects of information security ... and two thirds to non-technical matters ... [Jackson, 1990].

The use of technology in information systems has increased efficiency and effectiveness by untold orders of magnitude. Unfortunately, technology and the ease of access that it provides also creates security problems. The same technology which enables access to vast amounts of information can also be used to restrict access to that same information. "Ironically, the technology that has made possible much of today's

information dissemination retains a crucial role in safeguarding genuine privacy" [Behrens, 1985].

Policy stipulates some result desired by management and clear guidelines on how to achieve that result. Policy must be developed with a clear understanding of the items of value contained within the system, and with an understanding of the vulnerability to which these resources are exposed [Schweitzer, 1990]. The policy developed must be able to be used as a reference when circumstances require new or unusual courses of action.

> System security turns on often competing variables: the mandate of the agency; the sensitivity of the data; the consequences of data corruption; the level of commercial activity; manner of use; operational costs; and ease of access... Strenuous security requirements can impact negatively on the overall value of the information by reducing ease of access and positively on the protection of privacy [Kozub, 1991].

It appears that technology is best used to control the medium (i.e., the network) and the data, while policy has its optimal use in controlling people. Technology and policy must be used in concert to protect against abuses of information and invasions of privacy by individuals and organizations. It is essential to balance the requirement for civil liberties and access to information against the need for a secure, orderly and protected information society.

6. Access and Privacy Policy Development

In this chapter, legislation and policies that address information access and privacy will be reviewed. The assessment will progress from the whole to the part by first overviewing these issues as they apply to information in general. The scope will then narrow to concentrate specifically on land related information. Ultimately, an access and privacy policy development process for distributed land related information will be proposed.

As recognized by the Office of Technology Assessment [1988], most U.S. federal government agencies are operating in a partial policy vacuum when it comes to electronic information dissemination. It is likely that this situation is not unique to the U.S. or the public sector, but is to be found in all levels of society and in many countries. When it comes to electronic information policy, it can be seen from the preceding chapters that there are a multitude of factors to be considered, some of which are in conflict with each other. Enhancing public access, protecting privacy, minimizing inefficiency, optimizing the use of new technology, and defining the role of both the private and public sectors are just some of the issues at hand. Upon the introduction of any new variable, such as a distributed information environment, it is appropriate to reassess the purposes and goals of formal policies and procedures used to deal with access and privacy. If the implementation of access and privacy controls are to be altered, the policies and principles behind the implementations must be re-evaluated and clarified.

6.1. Generic Information

At present there is a significant body of legislation that is directed at general, not necessarily land related, government-held information. In our increasingly computerized information environment information knows no bounds, and yet much of the relevant legislation formalizes a distinction between the public and private sectors [Privacy Commissioner of Canada, 1991] and until recently has made a distinction between information stored electronically and information stored on hardcopy media. Information principles, on the other hand, tend to be more general and address information as an entity in its own right which should be viewed as a universal corporate resource.

6.1.1. Existing Legislation

6.1.1.1. Access

In countries such as Australia, New Zealand, Canada and the U.S. access to information is governed by detailed freedom of information statutes. Access legislation exists to provide a means by which government-held information may be made available to the public. Some of the idiosyncrasies of the legislation from these countries will be discussed below.

The Australian Freedom of Information Act, 1982, in a manner similar to the Canadian Access to Information Act, 1985, refers only to the release of documents. In both cases, the right to access extends only to the form in which the records or documents currently exist. There is no obligation to create a new record or document in response to a request. The similarity between the Australian and Canadian Acts continues, however, in that there is one exception to the preclusion of the creation of information to meet an access request, and that deals with data held in electronic form. Both Acts allow that if a record or document does not exist in a discrete physical form, but can be made to exist using the data, hardware, software and expertise existing within the government agency responsible for the data, then access must be provided.

The troublesome nature of requiring that information be embodied in physical documents or records has been avoided by the New Zealand Official Information Act, 1988. The N.Z. Act specifically provides for access to information rather than documents. It is possible, at the extreme, to request information which has not been recorded in any way, electronic or hardcopy, but is merely held in a government employee's head [Hazell, 1987a]. Despite the advantages of the wording of the N.Z. Act, in practice most people still tend to think of information as being physical documents or records [Hazell, 1987a].

The N.Z. Act is unique among the examples examined for yet another reason. It provides different rights of access to personal information than are offered for other official government information. Personal information is defined as that subset of official information held about an identifiable person. A statutory right of access is prescribed for access to personal information, whereas no such right exists for official non-personal information.

Both the Australian and N.Z. Act provide for the amendment of personal records that are inaccurate, incomplete or misleading. While part V of the Australian Act deals with the amendment of personal records, this section has largely been superseded by the advent of the Australian Privacy Act, 1988. The fact that access legislation contains substantial

sections dealing with the control of personal information highlights the complementary nature of privacy and access.

The Australian Freedom of Information Act seeks to allow access to all government-held information with the exception of specific exemptions. As stated above, in N.Z. access to official information is not based on a statutory right, and in addition, the range of exemptions which government may use to refuse disclosure is somewhat larger than those provided for personal information. The Canadian legislation provides access to information with exception provisions covering broadly the same range as those provided by the Australian and N.Z. legislation [Hazell, 1987b].

The main difference between the legislation from Canada and that from Australasia is that the Canadian Act does not provide for a 'balancing of public interest' test. A number of the exemptions in Australia and N.Z. require that the amorphous quality of 'public interest' be considered before access to information is denied. The absence of such a test may not be to Canada's disadvantage. The Australian Senate Standing Committee on Legal and Constitutional Affairs [1987] was of the opinion that the interpretation of public interest is one of the most difficult aspects of freedom of information decision making.

The Alaska Open Records Act, 1990, has been praised for its attempt to address electronic access to information and to strike a balance between cost recovery , access and privacy [Dansby, 1992]. The Act encourages government agencies to make information available in electronic formats to the greatest extent feasible. While the development of electronic access mechanisms is encouraged, the issue of equity of access is also well handled. Subsections f and h of section 09.25.115 state

> (f) When offering on-line access to an electronic file or data base, a public agency shall provide without charge on-line access to the electronic file or data base through one or more public terminals.
>
> (h) A public agency may not make electronic services and products available to one member of the public and withhold them from other members of the public.

The provision for online access to government databases by the Alaskan legislation certainly sets the pace for other access legislation. In defense of the Canadian legislation, that Act does state that its function is to complement existing information access procedures promoted by individual agencies rather than being the sole means by which information may be obtained. Access, as proposed by the Alaskan legislation, highlights the evolving

meaning of access to information (as defined in chapter 2 by ACUS). While information may be obtained only subsequent to a user initiated request, the desired information is readily available due to the provision of both data and the software necessary to enable enquiries.

A degree of consensus exists that freedom of information legislation applies to electronic information. There is, however, some disagreement over how far government should go in making its databases directly accessible to the public. Considering it has been estimated that within the next decade 80% of all public sector information will be stored electronically [Information Commissioner of Canada, 1991], it is necessary that any inadequacies in current access laws regarding electronic information be quickly and thoroughly addressed.

6.1.1.2. Privacy

The protection of privacy is without doubt an important issue for the well-being of society. On occasion, however, there may be circumstances where the need for an individual's privacy is outweighed by other societal claims. When such occasions arise there is a requirement for clear rules or guidelines detailing the conditions under which the violation of privacy can be supported. Privacy legislation is a compendium of such rules [Hazell, 1987b].

It would appear that privacy legislation in general is not suffering from technological obsolescence to the same extent as access legislation. There are several reasons for this. Firstly, privacy legislation deals only with personal information whereas access legislation attempts to cover the whole gamut of government-held information. Secondly, privacy legislation provides a general framework by which personal information and privacy may be addressed. The code of fair information practices that most legislation embodies does not become entangled in the specifics of technology or media. Typically such legislation refers to information rather than the media in which the information is stored. Whereas access legislation is couched in terms of documents and records, and then has to explicitly state what these mean and how they are to be interpreted in the case of computerization, privacy legislation is more general and hence more versatile.

This is not to say that media specific privacy legislation does not exist. For instance, both the U.S. Electronic Communications Privacy Act, 1986, and the Canadian Criminal Law Amendment Act, 1985, deal with the privacy of electronically stored and transmitted information.

The common root of the Australian Privacy Act, 1988, the Canadian Privacy Act, 1985, and much other privacy legislation of recent years lies in the OECD Guidelines. The Guidelines enunciate eight privacy principles which are regarded as a set of minimum standards [OECD, 1981]. The Australian legislation makes a point of clearly stating the principles upon which it is based (see appendix II for the information privacy principles found in the Australian Privacy Act). While the Australian Act contains eleven basic principles, a strong correlation exists between these and the eight OECD principles. The Canadian Act, although not stating the principles explicitly, does contain their equivalent throughout the body of the legislation.

In Australia and North America none of the privacy legislation is applicable to the private sector. In Canada such legislation has been enacted for all levels of government (federal, provincial and local) but, with the exception of legislation to regulate some of the activities of credit rating agencies and the like, no such legislation exists for the private sector. The situation in Europe is markedly different. The Europeans do not attempt to differentiate between the private and public sectors, but provide basic standards, such as the OECD Guidelines, that are universally applicable to control the dissemination and integration of information [Leia, 1989]. The U.K. Data Protection Act, 1984, is an example of information management legislation that applies to both the private and public sectors.

The U.K. Data Protection Act requires that any party maintaining a database containing information by which an individual may be identified must officially register as a 'data user'. The data user must provide a description of the data held and the purpose for which it is held, the source from where the information is obtained, the people to whom the information is intended to be released, and the countries to which the data is to be transferred. Once this meta data is registered the data user is not permitted to operate the database in any way other than that stated in the official register, i.e., cannot hold any personal data other than that stated, cannot use data for purposes other than those registered, cannot disclose information to persons other than those specified, etc.

Taken to the extreme the British legislation could prove onerous. It would seem that any data store containing personal information, regardless of its purpose, must be officially registered. Lists compiled by small business operators to help in the administration of their paper or milk round would be subject to the same requirements as data stores held by credit rating companies and government departments. The advantage of consistency is obtained at the cost of increased regulation and administrative overhead.

6.1.1.3. Complementary Nature of Privacy and Access

Despite the apparent antagonism between privacy and access legislation, it becomes clear upon closer inspection that the two are in fact complementary. Freedom of information legislation allows for access to all government-held information, subject to certain exemptions, one of which is based on privacy. Privacy legislation provides for control over one's own personal information, but recognizes that access to such information is justifiable in certain circumstances. The Canadian Privacy Act, for example, lists 13 circumstances under which personal information in the care of government may be disclosed.

The complementary nature of access and privacy is evidenced by legislation such as the Saskatchewan Freedom of Information and Protection of Privacy Act, 1991, and the Ontario Freedom of Information and Protection of Privacy Act, 1987, which combine the access and privacy issue into one piece of legislation. In these cases the hinge between the two concepts, the definition of personal information, is assured of being viewed consistently from both perspectives.

6.1.2. Proposed Legislation

At the legislative level, the United States appears to be pursuing the issue of access to information in an electronic environment with great vigour. There are currently at least six Bills before Congress that relate directly to access policy. Of these, three are of particular interest.

The three Bills, HR 3459 (Improvement of Information Access Act), S 1940 (Electronic Freedom of Information Improvement Act) and HR 2772 (Government Printing Office Wide Information Network for Data Online (GPO WINDO) Act) were all introduced in 1991. HR 2772 and S 1940 have a reasonable degree of political support, but HR 3459 has not attracted any co-sponsors to date. Much of the information provided about these Bills comes from electronic mail correspondence, mainly with Mr. James Love [1992].

HR 3459 was introduced in an attempt to broaden access to public information. It requires amendments to be made to the Freedom of Information Act. HR 3459 does not address the issues of what is to be collected and disseminated, but is aimed at ensuring free and ready access to information for the public. The basic assumption underlying the proposed legislation is that taxpayers paid for the creation, collection and organization of government information and therefore should not be required to pay excessive fees to receive and use that information.

The Bill seeks to improve public access to information by:

- specifically mandating government agencies to disseminate information, using computer technology if appropriate, and requiring agencies to provide adequate documentation, software, indexes and other resources to broaden public access;
- requiring the dissemination of information products and services in standardized record formats, and the development of a standard database query structure;
- limiting the cost of information products and services to the incremental cost of dissemination and prohibiting the imposition of royalty fees on the redissemination of information;
- requiring that government agencies engage in dialogue with the public in the form of public notice of discontinuation of information products, the development of new information services, etc.

S 1940 seeks to make amendments to the Freedom of Information Act to:

- direct agencies to publish certain of their information holdings electronically;
- include in that electronically published information set, meta data such as indexes, descriptions of new databases and instructions on how to use the databases;
- enable requesters to receive records in the format in which such records are maintained;
- require reasonable efforts by agencies to provide records in electronic form, even when such records are not usually maintained in that form;
- redefine the term 'record' to explicitly include electronic information, and redefine 'search' to include an automated examination to locate records.

S 1940 is attempting to strengthen the public's right to receive records, that are subject to disclosure under freedom of information legislation, in electronic format. The principle opposition to S 1940 comes from federal agencies trying to avoid their freedom of information responsibilities. This is in contrast to HR 3459, whose main opposition comes from commercial data vendors who fear competition from the enhanced access and improved scope and performance of government information products and services that the Improvement of Information Access Act would precipitate.

The Bill that has attracted the most Congressional support to date is HR 2772. This Bill, if enacted, will create low cost, one-stop-shopping, online access to federal government databases through a Wide Information Network for Data Online (WINDO) provided by the Government Printing Office (GPO).

The long term objective is to provide online access to as much federal information as possible, limited only by technological and economic feasibility. Through a single account citizens will be able to obtain, at cost, dial-up access to thousands of federal databases. WINDO will be used to complement rather than supplant the efforts of individual agencies to disseminate information. It is intended to increase the convenience with which the public may obtain access to government information. The development of standards, standard database query procedures, online help, user friendly interfaces, indexes and other meta data, are all part of the GPO WINDO proposal.

The above three Bills have been described as "the most positive statements about public access to [U.S.] federal information that have been introduced in Congress over the last decade" [Love, 1992]. GPO WINDO in particular appears to be very ambitious and offers exciting opportunities for public online access to information.

6.1.3. Existing Policies

Policies are used to place legislation and principles that exist about an issue in a particular context. Policies attempt to create a framework whereby objectives set by an organization can be achieved. In the U.S., the Office of Management and Budget (OMB) is authorized to provide guidance on information management, and does so through the publication of a series of circulars. OMB [1985] Circular A-130 addresses the issues of information privacy, access and dissemination for federal agencies. In Canada, at least two policy statements that have direct relevance to privacy and access have been developed by Treasury Board: the Management of Government Information Holdings Policy [Treasury Board of Canada, 1990a], and the Government Communications Policy [Treasury Board of Canada, 1990b].

6.1.3.1. Circular A-130

OMB Circular A-130 is a somewhat controversial information resource management policy [Office of Technology Assessment, 1988]. According to its detractors, who come mainly from the public sector, academic and librarian professions, "A-130 has a 'chilling effect' on government agencies' efforts to disseminate information in formats that citizens can use, such as online computer access to data" [Knaus, 1991]. It is charged that OMB has encouraged the privatization of information dissemination to an unhealthy extent.

A-130 does take a rather hard-line, but qualified, approach to the economics of information dissemination. It states that "public and private benefits derived from

government information, insofar as they are calculable, should exceed the public and private costs of the information." The policy then goes on to state,

> Although certain functions are inherently governmental in nature, being so intimately related to the public interest as to mandate performance by Federal employees, the government should look first to private sources, where available, to provide the commercial goods and services needed by the government to act on the public's behalf, particularly when cost comparisons indicate that private performance will be the most economical.

Although critics fear that A-130 places too much emphasis on the commodity nature of information and has lost sight of its 'public interest' value, there are many statements throughout the policy relating to the right to access and privacy. In particular, three of the twelve policy objectives deal with privacy and have direct parallels with the OECD Guidelines. In addition, the applicability of the Privacy Act and the Freedom of Information Act are reaffirmed as being pre-eminent in decisions relating to information access. There are many statements referring to the need to provide equitable access to the public and use of up-to-date information technology is encouraged to facilitate access and dissemination. A-130 mandates that public rights to access information derived from the Freedom of Information Act be preserved in electronic release systems.

6.1.3.2. Canadian Policies

The Canadian policies dealing with access and privacy have not attracted the criticism levelled against Circular A-130. Neither the Management of Government Information Holdings Policy nor the Government Communication Policy stress reliance on the private sector for dissemination of information to the same extent as A-130.

The elements that created dissent in the U.S. are, however, present in the Canadian policies. The Government Communications Policy clearly states that "the provision of information is costly and should only be undertaken where there is a clear duty to inform the public or where the user is willing to pay for it." There is also a requirement to consider contracting with the private sector, particularly for the provision of information from online databases.

Guidelines relating to assessing and defining information needs, collecting information, maintenance and protection of information resources, dissemination and use, and the preservation, retention and disposal of government information detail the responsibilities of government and largely reinforce many of the principles of the Access to Information Act

and the Privacy Act. The guidelines in the Management of Government Information Holdings Policy relating to dissemination state that "information holdings should be managed in a manner to facilitate public knowledge of and access to such holdings consistent with the principles ... of the Access to Information Act."

There is no doubt that public policy should attempt to promote diversity in electronic information products and services and hence increase information accessibility. There is also a need for checks and balances to ensure that qualities of importance to society, such as privacy, are protected. Both the U.S. and the Canadian policies recognize the power and value of electronically stored information; yet they are applied only to the control of government information. The situation in Europe is markedly different. Data protection controls over both the private and public sectors are common in many European Community countries. In North America, the private sector has been encouraged to voluntarily establish codes of fair information practice, particularly in relation to data privacy protection. To date very few private companies have responded to this encouragement [Privacy Commissioner of Canada, 1991].

6.1.4. Principles

The principles found in any society reflect the attitudes and values of that society. Principles, being broadly based, are applicable throughout society and are not delimited by artificially contrived barriers and boundaries The principles relating to information access and privacy may be reflected in legislation and may also find form in rules, regulations or guidelines.

Three sets of principles will be examined here. Firstly, Recommendation 88-10 of the Administrative Conference of the United States (ACUS) which addresses electronic acquisition and release of federal government information will be studied. Secondly, the principles set forth in 1990 by the Government Documents Round Table (GODORT) of the American Library Association with regard to government information will be commented upon. Lastly, the OECD Guidelines will be analysed.

6.1.4.1. ACUS

In December 1988 ACUS adopted a series of recommendations, known collectively as Recommendation 88-10, which address the use of computers in acquiring and releasing information by the U.S. federal government [ACUS, 1989]. The basic values underlying the ACUS recommendations differ very little from OMB Circular A-130, however, the ACUS recommendations do not presuppose who should add value to information (one of

the key complaints against Circular A-130) [Perritt, 1989a]. The text of Recommendation 88-10 is located in appendix III of this thesis.

ACUS recommendation A deals with the manner in which Freedom of Information Act obligations should be met in an electronic environment. The need for this recommendation stems from the lack of explicit recognition of electronic information in the current U.S. freedom of information legislation. It is suggested that electronically stored information be supplied to requesters in the form in which it is maintained or in any other form requested that can be readily produced using the data, existing software, and reasonable effort. Freedom of information legislation obligations are not to extend to the creation of large new databases to be used for private commercial advantage.

Recommendation B addresses the acquisition of information in electronic form. Electronic information acquisition is relatively non-controversial when compared with electronic information release [Perritt, 1989a]. The recommendation suggests that format standards be developed in consultation with information lodgers and that transition periods be provided to ease technologically unsophisticated users into the new mode.

The release of information in electronic form, covered in recommendation C, has considerable potential for controversy. At the heart of most of this controversy is the respective roles of the public and private sector in the dissemination of electronic information. Recommendation C suggests that agencies consider upgrading their level of information release from paper to electronic form, and from access to disclosure to dissemination.

Recommendation D addresses the allocation of responsibilities between public and private sectors. Pursuant to a decision to acquire or release information in electronic form appropriate roles for the public and private sectors must be defined. The qualities each sector has to offer, the services they are able to render, and the costs, both economic and non-economic, will determine the option chosen.

Emphasis is placed on carrying out cost benefit analyses to justify the changes suggested by recommendations B, C and D. An objective cost benefit analysis may be difficult to perform. Recommendation E states the costs and benefits that should be taken into account. Freedom of information obligations are included as a factor to be accounted for in the analyses.

Recommendation F urges that exclusive control over the acquisition and release of public information not be granted to any organization, private or public sector, in the absence of a compelling public purpose. Any desire to grant monopoly powers must be

measured against possible inconsistencies that may arise with regard to freedom of information responsibilities and the likelihood of inability to benefit from future technological developments.

Recommendation G requires that agencies stay abreast of technological developments and utilize the latest technology to provide appropriate levels of access and security. Existing information exchange standards are recommended in favour of developing individual and possibly incompatible proprietary formats. The use of public data networks is urged, rather than developing private communication links.

The remaining three recommendations deal with matters of an administrative nature. On the whole, Recommendation 88-10 provides a broad set of principles that can be used as a basis for policy development in any jurisdiction. The circumstances and expectations in any given jurisdiction will determine the specific nature of any subsequent policy.

6.1.4.2. GODORT

GODORT adopted eleven principles on government information in 1990 [GODORT, 1991]. Some of the principles are directed specifically at the U.S. federal government, but they are meant to be broadly applicable to all types of government information at all levels.

GODORT's principles are:

1. Access to government information is a public right that must not be restricted by administrative barriers, geography, ability to pay, or format.
2. The government has a responsibility to collect and disseminate information to the public.
3. Government information, including information in electronic form, should be disseminated in a manner and format that promotes its usefulness to the public.
4. Depository library programs must be preserved to provide equitable, no-fee access to government information for all citizens.
5. Cost of collecting, collating, storing, and disseminating government information should be supported by appropriation of public funds.
6. The role of private publishers should complement government responsibilities in the collection, storage, and dissemination of public information. Private sector involvement does not relieve the government of its information responsibilities.
7. Government information policy must ensure the integrity of public information. This policy should be determined by the chosen representatives of the people.
8. It is essential to safeguard the right of the government information user to privacy and confidentiality.

9. Government has an obligation to archive and preserve public information, regardless of format.
10. Government has a responsibility to provide a comprehensive catalog of all public information and services.
11. Copyright should not be applied to government information.

GODORT's principles clearly state that access to government information is an inherent right which must be provided equitably. Ability to pay and other factors, such as lack of technical expertise, should not be used to hinder access. GODORT recognizes that the private sector can complement the role of the public sector in providing access, but requires that government retain control of its corporate resource to ensure that the public value of the information is not jeopardized.

Although the bulk of GODORT's principles relate to information access, they also address the issue of privacy. In this respect they argue that the right of privacy must be extended to the information provider, as well as the information user. The appearance of this privacy requirement in the midst of a host of access requirements reinforces privacy as a right which is not necessarily contradictory to access. The two rights can co-exist without creating ambiguity.

6.1.4.3. OECD

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [OECD, 1981], state eight basic principles (located in appendix I) which form a minimum suggested standard to be adhered to when dealing with the privacy of personal data. These principles form the basis of much privacy legislation of recent years, e.g., Australia, Canada and the U.K. The Guidelines apply to personal data which "because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties" [OECD, 1981].

The collection limitation principle addresses two issues. The first issue dealt with is that personal data is somehow special and should be subjected to collection limitations. The limitations set may be developed from parochial privacy values pertaining to certain information, from civil rights concerns, or from concerns about appropriate uses of certain information by particular parties. In general, the amount of personal information collected should be limited to the minimum amount necessary for performance of a specified task. For instance, collection of information relating to marital status, religious beliefs, ethnic background, etc., would ordinarily not be necessary for the effective functioning of a land information system and is likely to be irrelevant to the purposes of the system.

The second issue deals with the manner in which information is gathered. Free and informed consent to collection of information is expected to be the norm, although exceptions are permitted 'where appropriate'. This clause might be used to cover collection of information for criminal investigation purposes or about mentally handicapped people.

The data quality principle recommends that data be of a quality adequate for the purpose for which it is collected. The accuracy, completeness and currency of information need only be assessed in light of intended uses. Information quality must be of a standard so that no harm is likely to be incurred by the information subject if the information is used for intended purposes. This principle appears to be restrictive in that better quality data would surely lead to greater utility. It must be remembered, however, that data is only intended to be used for those purposes initially specified, not for a wider audience.

For land related information the purpose specification principle poses some difficulties. When vast amounts of information are collected from large numbers of people and integrated with information collected at other times, to obtain system-wide efficiencies, it is often difficult to state exactly the purposes for which the information will be utilized. It is tempting to say that land related information is either public or non-personal and hence not subject to privacy protection principles. While this may be true for some land related information, it may also transpire that technological assistance enables identification of an individual from the data. In such a case, land related information must be regarded as personal and subject to the purpose specification principle.

The clause dealing with 'not incompatible' purposes may provide the solution in some instances. If the new use of information is in accord with the original intended purpose, such use is deemed to be legitimate. As long as the use of information contained in a land information system continues to be for the stated purpose of the system (e.g., land resource management) that use should be deemed acceptable.

The use limitation principle deals with the legitimate uses to which personal information may be put, and under what circumstances deviations from specified uses are permitted. Permission to use information for a purpose other than that initially specified may be obtained from the data subject, or under the authority of the law. The second source of authority recognizes that privacy is not an absolute right. Although personal information should be subject to strict controls regarding disclosure and use, there may be circumstances when the benefit to society of use of the data outweighs the loss of personal privacy. These circumstances will vary between jurisdictions, and will be reflected in the applicable legislation.

The security safeguards principle requires reasonable protection against improper use of information. As expanded upon in chapter 5 (security), the amount of security provided should be directly proportional to the value of the information or losses likely to be suffered should a security breach occur. Privacy, being a value of great importance in most societies, necessitates that a great deal of effort be put into securing personal information.

The openness principle requires data indexes to catalogue the existence of personal information. The indexes should provide a wide variety of meta data, such as the format of data, its location, its custodian, its attributes and uses, etc. This principle not only serves a useful purpose for privacy, but is vital for effective access.

The individual participation principle deals with the rights that an individual should be afforded with regard to accessing and challenging the correctness of personal information. This right is perhaps the most important privacy protection safeguard. While the Guidelines support the right to challenge the correctness of information held, they do not specify the exact remedy should a challenge be successful. The options of erasure, rectification, completion or amendment are suggested, but the action chosen is left to the discretion of the specific jurisdiction and the traditions and legislation applicable in that locale.

The accountability principle gives responsibility of compliance with the above principles to the data custodian. Custodial responsibilities do not cease when information leaves the direct control of the custodian. The custodian has a duty to protect information from misuse even when it is transferred to third parties. Contractual arrangements may have to be entered into to ensure information is properly and responsibly used.

The above Guidelines, although primarily interested in setting ground rules for privacy of personal data, occasionally overlap with access issues. This once again illustrates the degree to which these two issues are relevant to one another.

6.1.5. Summary

Principles, being representative of values and attitudes, must periodically be reassessed in light of changes to the environment in which they hold sway. It is hoped that principles, being general statements of societal ideals, will stand up to the test of time and adapt well to evolving applications, such as the introduction of new technology [Privacy Commissioner of Canada, 1990]. At some stage, however, principles must be translated into rules that can be applied to one particular set of circumstances (e.g., a certain class of people, information and activities).

When principles are used to produce policies, those policies must be developed with the understanding that:

- some flexibility or compromise may have to occur in order for consensus to be reached and a usable policy be produced for the community;
- existing statutes and regulations must be acknowledged;
- information access and privacy must be recognized as only two aspects of the broader information lifecycle.

6.2. Land Related Information

Land related information is a subset of the more general information addressed in the policies, principles and legislation outlined in section 6.1. As such it is reasonable to assume that the policies that apply to more general information also apply to land related information. Due to its specialized nature, however, land related information must also be subject to certain additional principles that apply specifically to this genre of information.

Traditions and values concerning land tend to be localized in nature. In response to this, policies used to control land information must also be parochial to a certain extent. Although variability in land information policy may occur between jurisdictions, the framework provided by general information principles provides a common basis.

6.2.1. Existing Legislation

Legislation relating specifically to access and privacy of traditional forms of land related information in electronic format is not very common. The U.S. is the main source of such legislation, particularly at the state level. Twenty five U.S. states have passed legislation that relates directly to geographic information systems (GIS) or issues that have become apparent due to the use of GIS [Dansby, 1992]. The legislation from two states, Kentucky and Iowa, will be used as examples of how access issues are dealt with for land related information.

The Kentucky Open Records Act, 1990, contains several sections that address access to government databases and GIS. Section 61.960 defines the terms 'database' and 'GIS'. These definitions place emphasis on electronically stored records that can be retrieved by computer.

Section 61.970 addresses the use of databases and GIS. The conditions under which provision of a copy of all or any part of a database are provided is dependent upon the intended use of the information. If the intended use is commercial in nature, the data is

deemed to be exempt from disclosure under the open records law. Such information may, however, be supplied subject to the requester agreeing to certain conditions. Firstly, the applicant must state the intended commercial purpose of the information. The user must then enter into a contract with the database custodian. Part of the contract will specify the fee to be charged for use of the data. The fee is determined by taking into account such factors as the cost to government of equipment, creation of the database, development overheads, etc., in addition to the likely commercial value of the information to the user.

Provisions are made, in section 61.975, for non-commercial access to information in electronic form. Subsection 2 states that information requested for non-commercial purposes will be provided in American Standard Code for Information Interchange (ASCII) format at a fee not to exceed the actual cost of copying, not including staff time. If the information requested requires a degree of customization or some alteration from the standard database product or services, the desired product or service will be provided, but at a cost which includes the cost of computer and personnel time and the cost of production.

Subsection 4 makes provision for remote access to a database or GIS. Such access requires the establishment of a license agreement or contract and the fees charged will include those costs incurred to provide the physical connection to the system and the cost of computer time access charges.

Interestingly, the Kentucky law provides an exemption from open records requirements for a large body of land related information. In section 61.960 (1) database is defined as "any group of records, electronically stored, that can be retrieved by a computer but shall not include electronically stored records of the Kentucky Geological Survey." To create such an exemption may be viewed by some as an inappropriate use of open record laws. The exemption of the Kentucky Geological Survey is similar to the U.S. federal Freedom of Information Act which includes as one of its nine disclosure exemptions geological and geophysical information concerning wells. At the federal level this exemption was established to protect proprietary and commercially valuable information compulsorily required to be lodged with government by private sector companies.

The Iowa Open Records Act, 1989, presents a stricter approach to permissible access to land related information. Section 22.2 (1) and (2) establish the right of every person to examine, copy and disseminate public records and the information contained therein. Furthermore, government is not permitted to contract with the private sector if such action prevents the public from examining and copying public records. Section 22.2 (3),

however, creates a condition of rigourous control over the release of electronically stored land related information.

> ... a government body which maintains a geographic computer data base is not required to permit access to or use of the data base by any person except upon terms and conditions acceptable to the governing body. The governing body shall establish reasonable rates and procedures for the retrieval of specified records, which are not confidential, stored in the data base upon the request of any person.

The rationale behind exempting electronic geographic data from disclosure under the open records law is unclear. There are those who would point to economic factors as the reason. When exemptions are made, care must be taken not to trivialize the legislation by including in it items that cannot truly be justified under the aim of the Act. Both of the Acts mentioned above deal with the issue of pricing at the same time that access is addressed. As the cost of providing electronic information is high and the commodity value of land related information is becoming more widely recognized it is likely that other jurisdictions will follow suit in stating economic considerations alongside those rights related to access.

6.2.2. Existing Policies

Policies aimed at land related information are more common than the existence of legislation covering the same topic. Policies dealing with access to land related information exhibit a reasonable degree of similarity regardless of their jurisdictional location. Some of this resemblance may be attributed to similarities in the way land information is typically used and the technology used to handle it. Adherence to like underlying access and privacy principles relating to general information may also account for some of the similarities.

6.2.2.1. United States

At the federal level the U.S. policy differs from countries such as Canada and Australia in that the U.S. government is not permitted to claim copyright on anything it produces. At the state level this restriction does not apply and the laws and policies regarding topics such as access to information are very much in keeping with those found in other common law countries. Most notably, some U.S. state governments have mandated recovery of costs, on a user-pays basis, for the distribution of land related information.

The state of Vermont has developed a Policies, Standards, Guidelines, and Procedures Handbook which includes a separate and detailed policy on public access to the products of

the Vermont Geographic Information System (VGIS) [Vermont Office of Geographic Information Services, 1991]. The policy has as its primary intent:

1. To provide VGIS access to the broadest possible base of users, constrained only by the availability of resources, and by the priorities identified to expand the development of data and applications most useful to VGIS users.
2. To define categories of access and customers.
3. To guarantee the integrity of all VGIS computerized data products.

Access to land related data provided by VGIS is currently available in electronic or hardcopy form, but access is not interactive. Access is only provided through the resources and staff of the Office of Geographic Information Services (OGIS). Access categories planned for the future include the full range of electronic graphic and non-graphic methods of data input, query and analysis.

The prioritizing of the development of geographic information products and access to these products appears to be one of the goals of the access policy. Policy statement M asserts:

> ... requests for services will be addressed on the basis of three criteria:
>
> 1. Whether provision of the requested service will help expand or hasten the identified priorities for data development within the VGIS.
>
> 2. Whether provision of the requested service will help expand the development of applications useful to constituent government units.
>
> 3. Any other.

It would seem that the access policy has built into it a market analysis function. This may help the OGIS in determining where to put the greatest effort in developing its market, but if the above policy statement is abused it may lead to access inequity by focusing the resources of the OGIS primarily on those activities which are financially rewarding.

The issue of competition with the private sector is dealt with by the statement that services for non-government customers will not be offered if private sector providers are able to meet the needs of the clients. An exception does exist if the service is deemed to be of benefit to data or application development. In such a case provision of the service may be considered despite the existence of a similar private sector service.

Johnson County, Kansas, has developed an access policy for its Automated Information Mapping System (AIMS) [Johnson County Planning Office, 1990] which has many of the same goals as the Vermont access policy, although it is worded in a way that implies that interaction with the private sector will be more strongly encouraged.

It is planned that AIMS information will be utilized as a readily available community resource in addition to providing benefits accruing from the more effective and efficient provision of government services. One of the stated goals of the policy is to establish "equitable arrangements for the shared development and use of AIMS products and services that are cost effective and revenue producing for the County."

The community resource facet of AIMS is intended to be developed by providing products and services that among other things:

- supply private sector commercial interests with readily available accurate and cost effective information;
- accommodate the needs and requirements of the public for governmental services or information;
- respond to requests and demands for information and products.

Access to AIMS information is made available in accordance with six user categories:

- general public access,
- county project access,
- inter-governmental access,
- public service access,
- private professional service access,
- private sector access.

Each user will be granted access to information at one of the following levels:

- orthophotograph copies and standard planimetric map plots,
- project-specific digital files,
- customized products and services,
- read-only access (online),
- full data sharing (online and data transfers).

Access and use of digital data is subject to license agreements. In accordance with the existence of copyright provisions, digital data is not permitted to be transferred to a third party, and is only to be used for the express purpose indicated by the requester.

The status of these two policies is on a par with those from other countries such as Canada. At this stage, development of the underlying databases is still underway and as a consequence part of the policy objective is to identify those areas that are showing the fastest growth rates, or the greatest potential, so that these needs may be met while aiding to accomplish some of the long-term goals of the overall project.

6.2.2.2. Canada

Policies relating to electronic access to land related information have been established by a number of Canadian provinces. Although some of these policies are relatively old, or were only intended as interim measures, little change has occurred in recent years. Although great activity is occurring in some provinces regarding online availability of land related information (e.g. Ontario, British Columbia, Manitoba) some of this activity is being guided by commercial pressures rather than explicitly stated access or privacy requirements.

The policy relating to electronic public access to government land data in Alberta [Government of Alberta, 1987] outlines several proposed access scenarios, including:

- copies of data on storage media (e.g., magnetic tape, magnetic disks, optical disks, etc.);
- on-line access to the data by a single agent or a limited number of agents or service bureaus, who provide direct electronic access through telecommunication links to end users on a fee-for-service basis;
- on-line access to the data by end users through telecommunication links; or
- broadcast of the data by satellite, with end users accessing the data through various reception technologies.

Privacy is addressed explicitly by this access policy, unlike the two American policies studied. The provision of online access is subject to the establishment of adequate security measures to ensure that data not intended to be publicly available is not able to be accessed. Such data could include all that which is exempt from disclosure under freedom of information legislation, in particular that of a private or confidential nature.

The manner in which data may be searched, a matter somewhat connected with privacy, is also addressed by the policy. The policy leaves it to the discretion of the custodian to determine if access should be provided to data in its raw form (i.e., searching capability provided only in a manner similar to the equivalent hardcopy product) or whether searches will be permitted on any of the data attributes.

The issue of value-adding and third party redistribution is ambiguous. The policy states that "data obtained ... may be used by the receiving organization for any legal purpose." This could be interpreted to mean that the redistribution of information obtained from government is permissible; that act in itself not being illegal. The procedures outlined by the policy state, however, that "all data which is distributed electronically will contain notice of copyright in the name of the originating department." This statement occurs in the section of the procedures dealing with liability. The specified minimum conditions to appear in any data use agreement appear to resolve the question, although there is still no explicit statement. One of the conditions to appear in any contract is to specify restrictions on the use of the data. Conceivably one of the restrictions could relate to redistribution.

The approach taken in Saskatchewan does not allow for such confusion. The Interim Policy on the Distribution of Digital Base Map Information [Saskatchewan Property Management Corporation, 1989] clearly states that a license agreement is to prohibit the redistribution of data or the distribution of value-added information without express permission. More recently, a variety of license agreements have been developed to suit the needs of different classes of users [George and Schlachter, 1990]. A third party license, for instance, permits a consultant to perform value-added work and to remarket that information, subject to the negotiation of a royalty agreement based on estimated sales and the proportion of original data content.

Although the controls placed on the use of digital information by the Saskatchewan policy appear to be quite strict, the primary role of the Central Survey and Mapping Agency should be kept in mind. That role is to "provide a cost recoverable land information product without restricting public access" [George and Schlachter, 1990]. This statement of access equity is fundamental to creating a strategic fit between the clients served, their capacity to pay, and their potential benefit from the use of digital land related information.

6.2.2.3. Australia

The Australian Surveying and Land information Group (AUSLIG)is the major producer and custodian of spatial data at the federal level in Australia. AUSLIG is responsible mainly for small and medium scale map data. This data is not available for

access online, but is available in a variety of magnetic media. AUSLIG is required to charge for the information it provides [Bell and Puniard, 1991].

Access to information is controlled by licensing agreements, which facilitate a two tier approach to the provision of non-exclusive data use rights. Non-exclusiveness is a feature of great importance if data monopolies are not to develop (although there is the fear that agencies such as AUSLIG may already be in a monopoly position). The first type of license is a standard license which allows the licensee to use the data only for internal purposes. The second type of license is a distributor's license which allows the licensee to sell or trade the data or any product derived from the data to a third party. The conditions set in the distributors license depend on the circumstances of each case, but license fees and royalty fees are generally levied [Bell and Puniard, 1991].

Information is made available to users at one of five levels. These levels relate to the degree of data quality. While the data dissemination activities of AUSLIG are largely driven by a full cost recovery motive, there is a responsibility to meet 'community service obligations'. Such public interest obligations are not required to be economically self supporting.

As the distribution of and access to data is mainly commercially driven, policies regarding access are not explicit. As freedom of information legislation cannot be utilized if information is publicly available, there is no recourse to this legislation. A proactive approach to the distribution of information renders freedom of information legislation unnecessary. The emphasis on the sale of land related information is growing and increasingly access is viewed in conjunction with marketing. This is evidenced by the development of a Marketing of Government Land Information Policy by the Western Australian Government [Government of Western Australia, 1992]. It is argued that marketing ensures the widest use and most convenient access to an information product.

The Western Australian policy also includes a very strong sentiment towards the right of privacy. The first policy statement enunciated is,

> Agencies shall not make available land information which contravenes individual privacy, commercial confidentiality, national security and information prohibited from release by existing W.A. law.

The policy clearly states that privacy and confidentiality are over-riding requirements and that trading in information should not take place at the expense of privacy and confidentiality. In W.A. the means of enforcing this policy is through the power of the

custodian agency. The custodian is responsible for seeing that information is collected, stored and used in an appropriate manner.

The main tool used to see that information is used in a manner that is deemed acceptable to the custodian is the license agreement. It is suggested by the W.A. policy that one of the first conditions in any data use agreement should address "intended and allowable use, privacy and confidentiality, national security interests and existing W.A. government legislative practises." The suggested policy conditions then go on to deal with the terms of access, including the right to redistribute the information to third parties and to develop and sell value-added information. The final statement of the policy asserts,

> Government will permit the licensing of its land information to the private sector for commercial purposes, including value-adding and on-selling providing the interests of privacy, commercial confidentiality and national security are protected.

The policy also addresses the issue of privacy when it states the factors that will be relevant when trying to discern to what degree the private and public sectors should be involved in the marketing of land related information. Two of the factors listed are:

- Privacy control – Public sector agencies are likely to be more receptive to the need for control than the private sector which may find itself in competitive situations where this may be compromised;
- Information security – Involving the private sector in collecting, maintaining as well as marketing land information could place the land information security in jeopardy due to changes in business ownership or the shift of the information offshore out of the reach of Australian legislation (especially privacy legislation).

Throughout the W.A. policy the provision of access is stressed as being best achieved through commercial means. The emphasis that is placed on maintaining control over the information to protect such qualities as privacy and confidentiality, therefore, is in contrast to the other policies studied. It shows a degree of recognition of the potential that land information may intrude on personal privacy that is lacking in the other policies. The fact that this policy is also the most recent perhaps tells the story. As institutional issues were, by and large, not addressed until technical matters were well in hand, so it is that privacy issues have not received a due proportion of attention until consideration of access issues are under way. It is a sign of the emphasis and priorities placed on the development of automated land related information systems.

6.3. Land Information Access and Privacy Policy Development

The development of a single access and privacy policy appropriate for all jurisdictions is a difficult, if not impossible, task. Variability in customs, values and laws prevent the crafting of a universally acceptable policy. When regulation of activities associated with information are contemplated, the codification process should take place subsequent to consideration of:

- the socio-political objectives to be met by information regulation;
- how regulation will fit into the social and traditional patterns of a jurisdiction;
- how advances in information technology will affect regulation [OECD, 1974].

While the jurisdiction dependant specifics of an information policy will not be discussed here, it is possible to isolate the elements which should be found in any policy if it is to adequately address access and privacy. Based on the land information policies studied and the ideals provided by access and privacy principles, it is possible to propose a set of components which should form a basis for any policy dealing with access and privacy to distributed land related information.

In addition to stating desirable components, strategies will be suggested that will increase the versatility of the final form of the policy. These strategies can be observed as inherent features of some of the principles studied. Their absence is responsible, in part, for the short-comings noted in some of the less serviceable policies and legislation. The strategies suggested should aid in the development of policies which adapt well to changes in environment (e.g., caused by the evolution of information technology) and prevent inconsistencies and discontinuities in the applicability of the policy.

6.3.1. Commitment to Information Access

The starting point of any access and privacy policy must be to declare a commitment to the control of information. The major emphasis in this statement should be placed on the word 'information' rather than 'control'. Too often policies devote their energies to the media on which information is stored rather than to the information itself. To permit decisions regarding the provision of information to be based on the medium rather than the information would allow the media to dictate policy. By adopting a media independent position, one policy can be applied consistently to all land related information.

Development of a land information access and privacy policy will fall between two extremes. One extreme entails stating the primacy of access and then qualifying this goal with exemptions, such as those relating to privacy. The opposite extreme involves placing

a blanket restriction on access to information, justified on such grounds as the proprietary nature of the information or privacy concerns, and then specify conditions under which access may occur.

Much of the land related information collected and held by government is not confidential, and is collected to provide a government mandated public benefit. The first priority of a government agency maintaining any form of information system containing public information must be to provide access to that information to effect the public benefit. In this case the commitment to access must be primary.

A clear indication of the manner in which an organization intends to view its information access responsibilities should be provided. If an affirmative approach to the provision of information is advocated, the extent to which the organization will go to meet user demands should be made clear. A commitment to the design and availability of information products and services should be made. In the case of agencies subject to freedom of information legislation, assurances should be given that although meeting the needs of users proactively will be a priority, the safety net provisions of open access legislation will still be available as an action of last resort.

Provision of access to information must be administered in accordance with the values and legislation of the jurisdiction. The policy developed must provide specific guidance on the issues of access and privacy as they relate to land information, but it must not conflict with existing legislation. Relevant legislation should be reinforced as having ultimate authority. The legislation to which the policy defers should be stated to give the user an indication of the broader social issues at play. For example, freedom of information and privacy legislation should be explicitly cited as having a predominant influence on the policy.

6.3.2. Access Mechanisms

Once statements regarding the degree of commitment to the concept of information access have been enunciated the means by which access may be obtained should be addressed. The tools used to aid and control information accessibility should be expounded.

One of the rationales behind operating in a distributed environment is to benefit from efficiencies gained through the sharing of information. Although the motives for government and the private sector may be different, the advantages sought through use of a network are common. Ease of communication translates directly into increased ease of access. Use of an electronic communication network is one means of realizing greater

access, but is only one option. The real goal is not use of a network, but use of any mechanism that improves access.

A commitment must be made to provide access to information in a manner that promotes its usefulness. In an information society, information is a valuable corporate resource with increasing tendencies to take on the form of a commodity in the marketplace. The commodity value of information is elevated if it is available in a manner that promotes its usefulness. The format in which information is available can act to promote and enhance usefulness. Different formats will have different utility to different users. Any policy adopted should not restrict itself by making statements about the media on which information will be made available.

Specification of various technical access categories may be useful. For instance, type of access (e.g., graphic query and plotting capability, non-graphic data input and analysis, graphic data input and analysis, etc.), user categories to be deployed (e.g., general public, inter-governmental, private sector, etc.) and privilege levels (e.g., read only, read and write, execute, etc.) are all means by which information access may be controlled. These are all forms of access and may be applied to specific media, but do not necessarily rely on a particular media. The specification of access forms should be handled with great care so as not to become technology dependant. If the technological environment changes it is important that the specified categories are not so dependant on the preceding technology as to become a hindrance in the face of change and render the policy a relic. Ideally the policy should remain applicable, appropriate and effective regardless of technological advances (but should always be sensitive to changes in societal values).

To foster a sense of stability and confidence in the user community a statement regarding standards should be formulated. Any attempt to develop organizational specific standards should be discouraged. Instead, industry standards should be advocated so that as the industry and its standards evolve, the organization will not be left in a situation where its products and services are increasingly marginalized and hence their usefulness diminished.

The policy should also contain some meta data regarding access mechanisms or a requirement for the collation of meta data. Meta data may exist in the form of a catalogue of both information and services. Such a catalogue should describe what information and services are available, where from, what equipment is necessary, how the information may be obtained, who is the custodian, why the information or service is provided (i.e., what is the intended purposed of its existence), what are the qualities of the information, etc.

6.3.3. Equity

The issue of access equity also warrants verbalization. If access class distinctions have been made it is particularly important to demonstrate equity within the user classes. A commitment to accommodate the information needs and requirements of all members of society must be offered.

A statement on access equity should address costs, convenience factors, geographic location, administrative barriers and technical requirements. Electronic access to information may alleviate some factors such as convenience and geographic location, as access is possible at any point where the network is in existence. Electronic access may, however, create inequity for those who are technologically disenfranchised due to cost or lack of expertise.

6.3.4. Privacy

The commitment to access must be accompanied by a similar commitment to privacy. While the desirability of access to information may have been stated first, this quality may be overridden if privacy rights are likely to be jeopardized as the result of release of information. The two qualities must be weighed in light of the circumstances in each case and there must be a balanced commitment to both access and privacy in all cases.

Policy statements concerning privacy must be developed within the confines of the parochial understanding of the term, and having due regard to existing legislation which addresses the issue. If no such legislation exists, or is deemed to be inadequate, reference to some other well founded principles of fair information dealing, such as the OECD Guidelines, should be made.

In keeping with guidelines such as those suggested by the OECD, there must be a commitment to ensure that any personal data over which the custodian has control is maintained in an accurate, current and secure state and that such information is of relevance to the operations of the custodian. These privacy considerations should be applied equally to all sectors of the community, public and private alike. The custodian as well as the information requester has an obligation to respect the right of privacy.

The concept of information privacy has more to do with controlling an individual's information environment than preventing collection or dissemination of personal information. So it is that the protection of information privacy is not aimed at preventing access to information so much as preventing an individual's right to privacy from being

infringed. If information is used in a manner that does not conflict with the controls desired by an individual then privacy is preserved.

Security safeguards are designed to protect the integrity, confidentiality and availability of information. The threats protected against are perceived attacks on the system, in one form or another. One possible threat to privacy, however, may come from the normal operation of an information system when information is voluntarily disclosed to a third party. This leads to a discussion of the legitimate use of personal information held in coincidence with land related information.

Uses to which information held in land information systems are put, typically have their emphasis directed towards analysis of land related information rather than personal data. When personal information is provided as an adjunct to land related information, to aid in the operation of the system, the subsidiary status of the personal data should be respected and maintained. To allow personal information to become the subject of analysis is likely a diversion from the purpose for which the information provider expected the information to be used. Such an activity would constitute a breach of information privacy.

There is a need for a statement regarding the legitimate use of land related information which contains personal information as attribute data. Such a statement should clarify the legitimate use of the database and privacy expectations. Decisions made about the appropriate use of personal information held in conjunction with non-personal land related information must be made in light of parochial values, the original intended use of the information, the proposed intended use of the information, the possible value to society as a whole, etc.

6.3.5. Security

Security is not the same as privacy and it is not the sole answer to protection of privacy. It does, however, provide many features which are useful in providing both privacy and access.

Security attempts to provide confidentiality, integrity, availability, utility and authenticity. These qualities increase the quality and value of information and are likely to be sought after when a user accesses information. These qualities would also seem to be of value in providing information privacy. The goal of information security, therefore, also serves as a useful component of access and privacy functions.

The presence of security functions, providing complementary services to both access and privacy, in addition to serving their own purpose, should be an obligatory component

of any information system. An access and privacy policy should state the importance of security to both access and privacy. The degree of security required should be commensurate with the risk and harm that would result from the loss , misuse or unauthorized access to or modification of information. The requirement for adequate security should be extended to the information user in addition to the custodian, especially for information held under license.

6.3.6. Information Ownership

The concepts of access and privacy as they relate to land information can only be comprehensively explained, and confusion about them avoided, if other satellite issues are also addressed. One such satellite issue is that of information ownership. The policy developed should clearly state who the information belongs to at all stages, so that responsibility for control of the resource is always clear.

Any statement regarding ownership of the information resource should include guidance as to:

- who owns the basic resource;
- what rights are transferred upon release of the information;
- the redistribution of information to third parties;
- the development of value added products from the basic information resource.

The policy should encourage equitable compensation for intellectual property owners (a must in the information age) but should not condone the existence of information monopolies, especially of government-held information, unless overriding concerns such as public benefit can be shown. Ownership (or custodianship) rights should be recognized but there must be a requirement that these rights not be abused to the detriment of information flows and the introduction of new, useful and appropriate technologies.

6.3.7. Pricing

Pricing is likely to be a very contentious issue and there will be great variability between jurisdictions, and even a large measure of dissent within jurisdictions. Whatever the strategy chosen, there must be a requirement that pricing not act to restrict public access or to cause inequity of access. The pricing strategy developed must conform to the requirement that it enable the widest possible access to information, by all members of society.

The pricing strategy developed should enable access to information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public. Included in the analysis to achieve this balance must be a full range of tangible and intangible costs and benefits.

6.3.8. Role of the Public and Private Sectors

To pre-empt any confusion and acrimony that may arise over the intended roles of the private and public sector in providing access to government information, the policy should indicate the role of each sector. It should also be recognized that the roles of each sector may change over time. Statements should be included supporting the complementary role that government and the private sector can play. It is clear that all sectors of society should be co-opted in the provision of information products and services in an attempt to encourage the development of a diversity of access avenues. This diversity is made all the more important because of the rapid rate of technological change and the lack of understanding of consumer preferences and the land information market in an information society in general.

Any access policy must recognize the existence of a multidimensional information services spectrum. Each element has qualities to contribute to maintaining access to information. Government must be cognizant of the need to fulfil mandated access provision functions and also be wary of providing information and services which are not within their mandate. Having satisfied their mandate as far as what is to be provided, the next question is how to facilitate that activity. There are certain mandated responsibilities regarding government-held land information for which the public sector must be held accountable. Even in these cases, however, it may be possible for the private sector to provide a supplementary role without necessarily pre-empting government's duties.

Factors that may play a role in determining what role any given sector will play in providing access functions include:

- the ability to ensure equitable and convenient access throughout the jurisdiction;
- the ability to enforce privacy controls;
- the availability of resources to meet user demands;
- the ability to maintain a secure environment for the information;
- the existence of special skills that will help meet the access needs and wants of the community.

6.3.9. Liability

In providing access to information there are certain responsibilities for which the custodian is liable. The custodian should make a commitment to data quality, including under that banner such features as maintenance of data integrity, accuracy and timeliness. The responsibilities of the custodian to provide information of an appropriate quality should be enunciated.

Custodians are also responsible for ensuring that the information under their care is not misused. Misuse of information may take many forms, but ultimately they can all be classified as the use of information for purposes never intended. If the information also contains personal data, misuse may result in a breach of information privacy.

The extent to which a custodian's liability extends may be difficult to define, especially when operating in a distributed information environment where information may be shared and interrelated with comparative ease. Data use contracts may help in specifying the limits of accountability as agreed upon by the parties to the contract.

6.3.10. Conditions of Use

The most widely used means of formalizing specific conditions of use of information, including those relating to access and privacy is through a data use agreement or contract. The statements contained in the policy should convey the desire that information not be misused in any way. It will likely be necessary to place access and privacy statements in any contract established.

The terms and conditions which typically form part of a data use agreement have been stated elsewhere (section 4.3.3.). The policy should contain some information regarding the elements likely to be found in the data use agreement. Some of those elements should relate to information access and privacy conditions.

6.3.11. Summary

It is unlikely that the development of any single policy will completely redress all information access and privacy concerns. By providing a concise, well reasoned formal statement of intents with regard to access and privacy, however, a commitment to these concepts is provided in a manner that can be relied upon. A summary of the components that should be found in any land information access and privacy policy is given in figure 8.

Advances in information technology are providing ever increasing means of gathering, storing, using and disseminating information about land. When, how quickly and at what

cost land related information becomes accessible is dependant upon the development of social, cultural, political and economic acceptance of the changes such access will precipitate [Behrens, 1985]. In turning general components of an access and privacy policy into specifics suitable for use in a certain jurisdiction the following are factors which will have some influence on the final form and content:

Commitment to Information Access

- Declaration of commitment to the control of information
- Statement of the priority placed on providing access to information products and services
- Affirmation of the importance of relevant legislation

Access Mechanisms

- Description of media independent access control categories
- Specification of technical standards addressing data format, exchange, enquiry, etc.
- Expression of commitment to the provision of meta data

Equity

- Pronouncement on the provision of equitable access to information

Privacy

- Statement of the importance of the value of privacy
- Declaration of the commitment to balance the qualities of access and privacy
- Declaration of the controls established to protect privacy
- Proclamation of the applicability of privacy provisions to all sectors and members of the community
- Recognition and application of privacy legislation and/or principles of fair information dealing
- Statement of the genre of intended, appropriate and accepteble uses of the information

Security

- Statement of appropriate security provisions
- Statement regarding the security responsibilities of custodians and information users alike

Information Ownership

- Declaration of the status of ownership of information
- Statement of the rights and responsibilities tranferred upon release of information
- Statement regarding the redistribution of information to third parties and the development of value-added products
- Description of public benefit factors to be proved if monopoly control of public information is proposed
- Expression of the balance to be maintained between ownership rights, information flows and equitable access

Pricing

- Declaration of the pricing strategy to be pursued
- Specification of the tangible and intangible costs and benefits to be considered in the provision of information

Role of the Public and Private Sectors

- Recognition of the qualities that the various sectors of the community possess that may prove beneficial in the development of a diversity of access avenues
- Enunciation of the roles that each sector may play and recognition that these roles may change over time

Liability

- Statement of custodial responsibilities
- Enunciation of the obligations of all parties to a data use agreement
- Statement of the limit of liability

Fig. 8. Components of an Information Access and Privacy Policy

- the resources available to develop land information products and services;
- the relative responsibilities and institutional arrangements within the public sector;
- the role of the private sector;
- the problems associated with coming to grips with developing technologies;
- the perception and legal status of social issues such as accessibility to the data, security of data, and privacy of the individual;
- the identifiable needs and priorities for land information;
- the impact that such information may have on society [Dale and McLaughlin, 1988].

The policy statements developed have intentionally attempted to stay media independent. This does not mean that the issue of information access and privacy in a distributed environment has not been addressed. On the contrary, it recognizes that a distributed environment removes many of the boundaries created by other media, such as paper, microfilm and even magnetic disks and tapes to a certain extent. Instead, the information available via a network is immediate to all users of the network and able to be used in any manner that those users please due to the power and diversity provided by information technology. Therefore it is essential that in addressing access and privacy in a distributed environment that it is truly the information that is being addressed rather than any specific media or physical manifestation. The physical manifestation of information is not constant. Information is the only real constant and so must be the prime focus of any policy.

There is a need to address land related information access in a proactive manner. If there is a requirement or a market for information, brought about by whatever reason, an active attempt should be made to make suitable information available. In an information society where information has a heightened value, such an approach can only benefit both the information provider and the user.

When considering the issues of access and privacy with regard to information it may be legitimate to consider them separately or in a linear fashion from a technological point of view. From a policy point of view, however, the two should be considered in concert. Certain elements exist within each of these issues that are affected by decisions made about elements in the other. The balance required between the two can only be struck if they are considered in coincidence.

The policy components suggested provide a framework for the development of a specific land information access and privacy policy. They also undertake to provide a strategy for avoiding inconsistencies and discontinuities that may occur if media specific solutions are attempted. The qualities of access and privacy, being so important to the development of a land information industry, should not be jeopardized by being confined to specific technologies. They should be applied in a balanced manner to information and to all sectors of society, having due regard to parochial values. The goal must be to maximize access to information to the greatest extent possible compatible with the preservation of the value of privacy.

7. Conclusion

Legal solutions developed to deal with traditional hardcopy information attempt to provide a balance between privacy and the right to access for that medium. Due to significant advances in technology, the legal framework and technological framework are no longer in complete harmony with regard to information access and privacy. Given the startling speed of technological change, it is difficult for the legal system to keep pace.

There is also a need to recognize that the changing role of information has an impact on the way it must be dealt with by policies. As information is increasingly viewed as a resource, a commodity and as property, attitudes toward its collection, storage and use change. Various responses to the changing perception of information can be witnessed. By and large, these responses have resulted in attempts to alter and amend existing legislation and policies. This approach is not adequate. Such a fundamental shift in the value of information warrants a substantial redrawing of policies of consequence to information access and privacy.

The power of computers, the growing abundance of databases, and the potential ease of access to those data stores, combine to create a disturbing scenario. The ease with which relatively innocuous individual data sets, even land related data, can be combined to create information which could be regarded as an invasion of personal privacy, is only too obvious. The increasingly sophisticated capabilities of technology highlight the inadequacies of existing access and privacy policies. These inadequacies are particularly apparent when private sector collection, dissemination and use of information is examined.

This thesis has proposed a set of components that should be present in any policy seeking to address access and privacy. The set is intentionally non-specific and is intended as a guide for use in any jurisdiction rather than as a ready-to-use policy for any particular community. It is recognized that the components suggested may not be exhaustive. They attempt, however, to address only those issues that have a direct impact on access and privacy. In formulating a general land information policy a broader range of topics will necessarily be covered.

In addition to the policy components a strategy has been suggested for the development of access and privacy policy. The strategy is imbedded in the wording of the components for the most part. The major thrusts which are felt to be important for land related information include:

- media independence;

- applicability to all sectors;
- encouragement of proactive information dissemination;
- coincident consideration of privacy.

By eliminating dependence on specific media, policies can be developed which take into account the continuing advances in technology and be flexible enough to accommodate these advances. Flexibility in this sense does not mean that the policies be 'wishy-washy' in their statement of what is acceptable and what is not. Flexibility in policies must be achieved by dealing with the underlying issues associated with information, rather than any physical manifestation or technology. For instance, the regulation of technology itself would serve little purpose. It is the use of technology and the use of the products of that technology that must be regulated if the greatest benefit and effectiveness is to be achieved. There is little point in regulating the media through which information is created, stored or disseminated. It is more to the point to regulate the information and its use. By adopting such an approach it is hoped that the policy will be able to evolve with technology and society and remain effective, appropriate and applicable.

Information privacy, in particular, is a concept that demands equal adherence by all sectors of society. Regardless of the motives for providing access to information, privacy is a right that must be respected by all parties. Consistent application of information access regulation across all sectors is more complicated. Government and the private sector are generally driven by mandates that require a different emphasis to be applied when considering access. There are, however, some aspects of access which are common to all sectors. For instance, the objectives of increasing the ease of access to information, providing information with the appropriate degree of utility, and increasing the land information market, are objectives likely to be pursued by all information providers. To aid in attaining these goals, and others, there is a need for cooperation and coordination between all sectors. The interests of information providers located at all levels in all sectors must be balanced with those of society.

In accord with the cooperation of the sectors for the mutually beneficial development of the land information marketplace, a proactive approach to the dissemination of information is suggested. As the market is not yet well known, the best strategy may be to encourage a diversity of information products and services from all sectors. The market will ultimately reveal those products and services that are of greatest value to society. The public sector has a special role to play in the development of this strategy. It must walk the thin line between providing information for the public benefit, attempting to ensure equity of access,

and yet not place itself in direct competition with the private sector. As information is made more widely available an increased exposure to liability will be encountered. This increased exposure will come from a wider class of user, using the information for an increasing range of tasks, with a greater expectation of quality. The potential for liability must be carefully managed, but should not be permitted to overshadow the advantages to be gained by providing increased accessibility to information.

Finally, privacy must be considered in coincidence with all access decisions. The important point to recall is that privacy acts to provide controls over information so that personal autonomy, dignity and liberty are not breached. It is personal privacy that must be protected when controlling collection, access and use of information, not a misplaced emphasis on the restriction of access to data. Although information technology blurs the distinction between personal information (i.e., that which can be used to identify an individual) and non-personal land related information, emphasis must be placed on the use of information for its original (or not incompatible) purpose. Such a use is likely to result in adherence to the concept of free and informed consent for the use of information, and hence privacy will not be breached.

As improved access is sought by both information providers and users, and the potential for breaches of privacy subsequently rises, the role of security will become increasingly important. The functions provided by a security system assume added value as the latent security offered by hardcopy media evaporates with increasing use of information held in distributed environments. Security will play a key role in the provision of both access and privacy at a level of liability acceptable to all parties concerned in an information transaction.

At the heart of the matter it can be seen that access and privacy have similar underlying social objectives. They are both qualities that are necessary if individuals are to participate and contribute in society and still maintain a degree of personal autonomy and integrity. Both qualities are necessary for the development and continuance of a free and democratic society. In formulating any land related information access and privacy policy free from inconsistencies and discontinuities, all of the development strategies suggested will likely be intertwined as they address the matter at hand. The success achieved by any such policy will largely depend on how well it maintains the appropriate balance between access and privacy.

References

ACUS (1989). "Recommendation 88 -10." *Federal Register*, Vol. 54, No. 21, February, pp. 5209 – 5212.

Alberta Land Surveyors' Association (1991). "A position on issues relating to unauthorized use of information, liability and privacy in the Information Economy."

ALIC (1990a). "Data Custodianship/Trusteeship." *Issues in Land Information Management, Paper No. 1.* Australian Land Information Council, Belconnen, A.C.T.

ALIC (1990b). "A General Guide to Copyright, Royalties and Data Use Agreements." *Issues in Land Information Management, Paper No. 2.* Australian Land Information Council, Belconnen, A.C.T.

ALIC (1990c). "Charging for Land Information." *Issues in Land Information Management, Paper No. 3.* Australian Land Information Council, Belconnen, A.C.T.

ALIC (1990d). "Access to Government Land Information – Commercialisation or Public Benefit?" *Issues in Land Information Management, Paper No. 4.* Australian Land Information Council, Belconnen, A.C.T., December.

ALIC (1990e). "National Strategy on Land Information Management." Australian Land Information Council, Belconnen, A.C.T.

Anderson, R.I. and R.A. Moore (1991). "SURVUS Project." Unpublished report of the Department of Surveying Engineering, University of New Brunswick, Fredericton, N.B., Canada.

ANZLIC (1992). "Privacy, Confidentiality and Access to Information in Land Information Systems." Third draft of proposed *Issues in Land Information Management, Paper No. 5.* Australian and New Zealand Land Information Council, Belconnen, A.C.T.

Archer, H. (1988). "Providing and Selling Access to AM/FM Data: Case Studies." *Proceedings of the 1988 Annual Conference of URISA. Mapping the Future,* Vol. IV, Ed. L.C. Williams. Los Angeles, California, U.S.A., 7 – 11 August, pp. 348 – 357.

Australian Senate Standing Committee on Legal and Constitutional Affairs (1987). *Freedom of Information Act, 1982. Report on the operation and administration of*

the freedom of information legislation. Australian Senate, Canberra, Australia, December.

Bayne, P.J. (1984). *Freedom of Information.* The Law Book Company, Sydney, N.S.W.

Behrens, J.O. (1985). "Accessibility of Public and Private Land Information – New Departures for Old Realities." *Proceedings of the 1985 Annual Conference of URISA. Computers in Public Agencies, Sharing Solutions,* Vol. I, Ed. B.J. Niemann, Jr. Ottawa, Ontario, Canada, July 28 – August 1, pp. 11 – 28.

Bell, G. (1988). "Third Party Information: Too Many Protections? or Too Few?" Proceedings of *Key to the 90s: Privacy and Information Access.* Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 16 – 19.

Bell, K.C. and D.J. Puniard (1991). "Digital Data for Land/Geographic Information Systems: Off-the Shelf or Do-it-Yourself?" *Proceeding of LIM Conference,* Ed. E.G. Masters and J.R. Pollard. Sydney, N.S.W., 10 —11 July. School of Surveying Monograph No. 14, University of New South Wales, Kensington, N.S.W., Australia, pp. 13 – 20.

Berman, J.J. (1989). "The Right to Know: Public Access to Electronic Public Information." *Software Law Journal,* Vol. 3, Summer, pp. 491 – 530.

Branscomb, A.W. (1988). "Who Owns Creativity? Property Rights in the Information Age." *Technology Review,* Vol. 91, No. 4, May/June, pp. 38 – 45.

Branscomb, A.W. (1986). "Law and Culture in the Information Society." *The Information Society.* Vol. 4, No. 4, pp. 279 – 311.

Budd, R.W. (1987). "Limiting Access to Information: A View from the Leeward Side." *The Information Society.* Vol. 5, No. 1, pp. 41 – 44.

Burkert, H. (1987). "A Functional Approach to the Legal Rules Governing Secrecy and Openness." *Proceedings of the Seventeenth Colloquy on European Law – Secrecy and Openness: Individuals, Enterprises and Public Administrations.* Council of Europe, Zaragoza, Spain, 21 – 23 October, pp. 10 – 50.

Burshtein, S. (1987). "Copyright and Useful Articles." *Engineering Digest,* Vol. 33, January, p. 29 and February, pp. 39 – 41.

Campbell, B. (1980). "Third Party Liability of Surveyors and Confidentiality of Survey Records." *Association of Ontario Land Surveyors Annual Report*, 20 – 21 February, pp. 142 – 157.

Campbell, F.H.A. (1991). "Cost vs. Revenue – How Much is Enough." *Conference of Commonwealth Surveyors 1991*, Paper No. B1.

Cavoukian, A. (1988). "Privacy: Some Comparative Issues and What the Future Holds." Proceedings of *Key to the 90s: Privacy and Information Access*. Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 135 – 138.

Chartrand, R.L. (1987). "Public Laws and Public Access." *The Information Society*, Vol. 5, No. 1, pp. 7 – 18.

Chatterton, W.A. and E.F. Epstein (1984). "Legal Issues in the Development of Land Information Systems." Seminar on the Multipurpose Cadastre: Modernizing Land Information Systems in North America. Ed. B.J. Niemann Jr. Institute for Environmental Studies Report 123. Wisconsin Land Information Reports: Number 1, University of Wisconsin – Madison, U.S.A., December, pp. 203 – 209.

CLIC (1990). "Electronic Legal Information: Exploring Access Issues." Report prepared for Canadian Legal Information Centre, Ontario, by K. Kelso, Alamar Education Incorporated, Ontario, April.

Cuming, R.C.C. (1991). "Implications of Unauthorized Use of Data in Specified British Columbia Government Data Banks." Report prepared for the Corporate and Personal Property Registries Branch, Ministry of Finance and Corporate Relations, British Columbia, Canada, August.

D'Elia, G. and L.F. Lunin (1991). "Perspectives on Integrated Information Centres Within Academic Environments." *Journal of the American Society for Information Science*, Vol. 42, No. 2, March, pp. 116 – 151.

Dale, P.F. and J.D. McLaughlin (1988). *Land Information Management: An Introduction with Special Reference to Cadastral Problems in Third World Countries*. Clarendon Press, Oxford.

Dando, L.P. (1991). "Open Records Law, GIS, and Copyright Protection: Life after Feist." *Proceedings of the 1991 Annual Conference of URISA. Information and Technology: Gateway to solutions,* Vol. IV, Ed. R.J. Anderson. San Francisco, California, U.S.A., 11 – 15 August, pp. 1 – 17.

Dansdy, H.B. (1992). "Survey and Analysis of State GIS Law." *GIS Law*, Vol. 1, No. 1, pp. 7 – 13.

Dansby, H.B. (1991). "Informational Privacy and GIS." *Proceedings of the 1991 Annual Conference of URISA. Information and Technology: Gateway to solutions,* Vol. IV, Ed. R.J. Anderson. San Francisco, California, U.S.A., 11 – 15 August, pp. 18 – 28.

Davies, K.J. and K.J. Lyons (1991). "Micro-Economic Reform, Land Administration, and Land Information Management." *Proceeding of LIM Conference*, Ed. E.G. Masters and J.R. Pollard. Sydney, N.S.W., 10 —11 July. School of Surveying Monograph No. 14, University of New South Wales, Kensington, N.S.W., Australia, pp. 87 – 96.

Department of Communications (1984). *Copyright and the Cultural Community.* Govt. of Canada, Ottawa, May.

Department of Defense (1985). "Trusted Computer Systems Evaluation Criteria." DoD 5200.28-STD, United States, December. In Parker, D.B. (1991). "Restating the Foundation of Information Security." *Datapro Reports on Information Security*, IS09-125, November, pp. 101 – 109.

Department of Justice (1987). *Access and Privacy: The Steps Ahead.* Ottawa, Ontario, Canada.

Doctor, R.D. (1991). "Information Technologies and Social Equity: Confronting the Revolution." *Journal of the American Society for Information Science*, Vol. 42, No. 3, April, pp. 216 – 228.

Donahue, J.D. (1989). *The Privatization Decision – Public Ends, Private Means.* Basic Books, Inc. New York.

Economic Council of Canada (1971). *Report on Intellectual and Industrial Property.* January.

Elmasri, R. and S.B. Navathe (1989). *Fundamentals of Database Systems.* The Benjamin/Cummings Publishing Company, Inc. Redwood City, California, U.S.A.

Epstein, E.F. (1992). Presentation at a seminar on institutional issues related to access to public databases. Fredericton, New Brunswick, 22 January.

Epstein, E.F. (1990). "Access to Information: Legal Issues." Proceedings of the XIX Congress of FIG. Helsinki, Finland, 10 – 19 June, Comm. 3, pp. 91 – 99.

Epstein, E.F. and H. Roitman (1987). "Liability for Information." *Proceedings of the 1987 Annual Conference of URISA. Building on the Past – Shaping the Future,* Vol. IV, Ed. M.J. Salling and L. Taylor. Fort Lauderdale, Florida, U.S.A., 2 – 6 August, pp. 115 – 125.

Fitzsimmons, J.J. (1987). "The Information Millenium." *The Information Society.* Vol. 5, No. 1, pp. 51 – 55.

Flaherty, D.H. (1991). "On the Utility of Constitutional Rights to Privacy and Data Protection." *Case Western Reserve Law Review,* Vol. 41, pp. 831 – 855.

Flaherty, D.H. (1988). "Privacy: Some Comparative Issues and What the Future Holds." Proceedings of *Key to the 90s: Privacy and Information Access.* Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 132 – 135.

Fox, G.G. (1976). "Institutional Impacts of Introducing Information Technology at the Local Level." *Symposium on Information Technology and Urban Governance.* Ottawa, Ontario, Canada, 24 – 26 February.

George, J. and R. Schlachter (1990). "A Financial Model for a Provincial GIS: The Saskatchewan Experience." *Presented at the 1990 Annual Conference of URISA. Information: The Currency of the Future.* Edmonton, Alberta, Canada, 12 – 16 August.

Glenn, P. (1989). "The Non-Technical Risks Associated with Implementing an LRIS Network." *Proceedings of the 1989 Annual Conference of URISA. Charting the 90s: New Visions for Urban Technology,* Vol. IV, Ed. W.F. Gayk. Boston, Massachusetts, U.S.A., 6 – 10 August, pp. 175 – 181.

Globe and Mail (1990). "Disasters get Bigger as Tech Goes Higher." November 12.

GODORT (1991). "GODORT's Principles on Government Information." *Documents to the People*, Vol. 19, March, pp. 12 – 14.

Gould, C.C. (1989). "Network Ethics: Access, Consent and the Informed Community." In *The Information Web: Ethical and Social Implications of Computer Networking*, Ed. C.C. Gould. Westview Press, Boulder, U.S.A., pp. 1 – 36.

Government of Alberta (1987). Policy and Procedures for Electronic Public Access to Government Land Data. Edmonton, Alberta, Canada, April.

Government of New Brunswick (1989). New Brunswick Land Information Policy. Fredericton, New Brunswick, Canada, March.

Government of Western Australia (1992). Marketing of Government Land Information Policy. Perth, Western Australia, February.

Halliden, P. (1990). "Network Security Issues." *Computer Communications*, Vol. 13, No. 10, December, pp. 626 – 629.

Halpern, S.W. (1990). "The 'Inviolate Personality' – Warren and Brandeis After One Hundred Years: Introduction to a Symposium on the Right of Privacy." *Northern Illinois University Law Review*, Vol. 10, Summer, pp. 387 – 399.

Hamrin, H.D. (1981). "The Information Economy: Exploiting an Infinite Resource." *Communications Tomorrow – The Coming of the Information Society*, Ed. E. Cornish. World Future Society, Bethesda, M.D., U.S.A., pp. 66 – 71

Hart, T. (1991). "Land Information Management; The Institutional Issues." *Proceeding of LIM Conference*, Ed. E.G. Masters and J.R. Pollard. Sydney, N.S.W., 10 —11 July. School of Surveying Monograph No. 14, University of New South Wales, Kensington, N.S.W., Australia, pp. 115 – 124.

Hazell, R. (1987a). *Report to the Cabinet Office (M.P.O.) on the Operation of the Official Information Act in New Zealand.* March.

Hazell, R. (1987b). *Report to the Cabinet Office (M.P.O.) on the Operation of the Access to Information and Privacy Legislation in Canada.* August.

Hendricks, E. (1988). "Computer Matching." Proceedings of *Key to the 90s: Privacy and Information Access*. Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 96 – 98.

Hernon, P. and C.R. McClure (1984). *Public Access to Government Information: Issues, Trends and Strategies*. Ablex Publishing, New Jersey, U.S.A.

Hondius, F.W. (1987). Opening speech. *Proceedings of the Seventeenth Colloquy on European Law – Secrecy and Openness: Individuals, Enterprises and Public Administrations*. Zaragoza, Spain, 21 – 23 October, pp. 6 – 9.

Information Commissioner of Canada (1991). *Annual Report of the Information Commissioner, 1990 – 1991*. Office of the Information Commissioner of Canada, Ottawa, Ontario, Canada, June.

Jackson, C.B. (1990). "The Need for Security." *Datapro Reports on Information Security*, IS09-100, October, pp. 101 – 134.

Janson, P.A. and R. Molva (1991). "Security in Open Networks and Distributed Systems." *Computer Networks and ISDN Systems*, Vol. 22, No. 5, October, pp. 323 – 346.

Johnson, W.R. (1991). "Anything, Any time, Anywhere: The Future of Networking." in *Technology 2001: The Future of Computing and Communications*, Ed. D. Leebaert. MIT Press, Cambridge, Massachusetts, U.S.A., pp. 150 – 175.

Johnson County Planning Office (1990). Access Policy and Interim Access Procedures. Johnson County, Kansas, U.S.A., March.

Jones, M.G. (1984). "The Advent of the Information Age: What's at Stake for Consumers." *Proceedings of the Seventh International Conference on Computer Communication. The New World of the Information Society*, Eds. J.M. Bennett and T. Pearcey. Sydney, N.S.W., Australia, October 30 – November 2, pp. 466 – 473.

Kahin, B. (1991). "Information Policy and the Internet: Toward a Public Information Infrastructure in the United States." *Government Publications Review*, Vol. 18, No. 5, September/October, pp. 451 – 472.

Knaus, H. (1991). "Facts for Sale." *Multinational Monitor*, Vol. 12, No. 5, May, pp. 26 – 28.

Kozub, N.E. (1991). "An Exercise in Strategic Planning: Development of Data Policy for the Information Age." *Proceedings of the 1991 Annual Conference of URISA. Information and Technology: Gateway to solutions,* Vol. IV, Ed. R.J. Anderson. San Francisco, California, U.S.A., 11 – 15 August, pp. 39 – 49.

Land Information Steering Committee (1990). "Pricing and Distribution of Digital Land Information." Discussion paper prepared for the Ministry of Crown Lands. Victoria, British Columbia, Canada, April.

Lawrence, J. (1990). "The Economics of Pricing GIS Products." *Proceedings of the 1990 Annual Conference of URISA. Information: The Currency of the Future,* Vol. II, Ed. W.J. Bamberger and G. Trobia. Edmonton, Alberta, Canada, 12 – 16 August, pp. 87 – 96.

Lee, Y.C. and J.D. McLaughlin (1991). "Distributed Land Information Networks: Database Management Issues." *CISM Journal*, Vol. 45, No. 3, Autumn, pp. 353 – 363.

Leia, G.J. (1989). "Telematics: Canadian Legal Response to Issues of Privacy and Confidentiality." *Proceedings of the 1989 Annual Conference of URISA. Charting the 90s: New Visions for Urban Technology,* Vol. IV, Ed. W.F. Gayk. Boston, Massachusetts, U.S.A., 6 – 10 August, pp. 277 – 292.

Linden, S. (1988). "Emerging Privacy Issues." Proceedings of *Key to the 90s: Privacy and Information Access.* Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 88 – 95.

Love, J. (1992). Communication via Internet, both personal and through various email discussion groups. Director of Taxpayer Assets Project, Princeton, New Jersey.

Lyon, D. (1988). *The Information Society: Issues and Illusions.* Polity Press, Cambridge.

Macartney, C. (1988). "Information Resources Management: Additional Costs or Additional Benefits." Proceedings of *Key to the 90s: Privacy and Information Access.* Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 29 – 33.

MacLean, D.J. (1984). "Leviathan in Lilliput: Patterns of Political Control in the Information Society." *Proceedings of the Seventh International Conference on Computer Communication. The New World of the Information Society,* Eds. J.M. Bennett and T. Pearcey. Sydney, N.S.W., Australia, October 30 – November 2, pp. 452 – 457.

Mann, J.F. (1987). *Computer Technology and the Law in Canada.* Carswell, Toronto, Canada.

McBride, A. and S. Brown (1991). "A Multi-Dimensional Look at the Future." in *Technology 2001: The Future of Computing and Communications,* Ed. D. Leebaert. MIT Press, Cambridge, Massachusetts, pp. 176 – 204.

McLaughlin, J.D. (1991). *Land Information Management I.* Department of Surveying Engineering, notes from lecture series SE6501, University of New Brunswick, Fredericton, N.B., Canada.

Melody, W.H. (1981). "the Economics of Information as Resource and Product." *Proceedings of the Pacific Telecommunications Conference,* Ed. D.J. Wedemeyer. Honolulu, Hawaii, U.S.A., 12 – 14 January, pp. C7 5 – 9.

Milliken, M.D. (1990). Distributed Computing Environments." *Patricia Seybold's Network Monitor,* Vol. 5, No. 1, January.

Mitchell, J. (1990). "Nowhere to Hide." *Globe and Mail, Report on Business*, May.

Moffett, J., M. Sloman and K. Twidle (1990). "Specifying Discretionary Access Control Policy for Distributed Systems." *Computer Communications*, Vol. 13, No. 9, November, pp. 571 – 580.

Moor, J.H. (1989). "How to Invade and Protect Privacy and Computers." In *The Information Web: Ethical and Social Implications of Computer Networking*, Ed. C.C. Gould. Westview Press, Boulder, U.S.A., pp. 57 – 70.

National Commission on Libraries and Information Science (1990). "Principles of Public Information: A Major Federal Policy Document from NCLIS." *Information Hotline*, Vol. 22, October, p. 5.

Nickel, J.W. (1989). "Computer Networks and Normative Change." In *The Information Web: Ethical and Social Implications of Computer Networking*, Ed. C.C. Gould. Westview Press, Boulder, U.S.A., pp. 161 – 176.

OECD (1983). *An Exploration of Legal Issues in Information and Communication Technologies*. Organisation for Economic Co-operation and Development Publications Office, Paris.

OECD (1981). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. No. 8 of the Information Computer Communication Policy series. Organisation for Economic Co-operation and Development Publications Office, Paris.

OECD (1976). *Policy Issues in Data Protection and Privacy*. No. 10 of the Informatics Studies series. Organisation for Economic Co-operation and Development Publications Office, Paris.

Office of Management and Budget (1989). "Second Advance Notice of Further Policy Development on Dissemination of Information." *Federal Register*, Vol. 54, No. 114, June 15, pp. 25554 – 25559.

Office of Management and Budget (1985). "Circular A-130." *Federal Register*, Vol. 50, No. 247, December 24, pp. 52729 – 52751.

Office of Technology Assessment (1988). *Informing the Nation: Federal Information Dissemination in an Electronic Age*. Prepared for the United States Congress, Washington, D.C., October.

Office of Technology Assessment (1986). *Federal Government Information Technology: Electronic Record Systems and Individual Privacy.* Prepared for the United States Congress, Washington, D.C., June.

Office of Technology Assessment (1982). *Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity.* Background paper prepared for the United States Congress, Washington, D.C., March.

Onsrud, H.J. (1990). "Liability Concerns for Surveyors." *ACSM Bulletin*, April, No. 125, pp. 20 – 24.

Parker, D.B. (1991). "Restating the Foundation of Information Security." *Datapro Reports on Information Security*, IS09-125, November, pp. 101 – 109.

Parker, D.B. (1989). "The Ethics of Voluntary and Involuntary Disclosure of Company-Private Information." In *The Information Web: Ethical and Social Implications of Computer Networking*, Ed. C.C. Gould. Westview Press, Boulder, U.S.A., pp. 259 – 268.

Penfound, R.C. (1990). "Survey Plans, Copyright and Government Process in the Maritimes: Ownership and Use of Plans and Third Party Liability." *CISM Journal*, Vol. 44, No. 3, Autumn, pp. 257 – 262.

Perritt, H.H. (1990). "Federal Electronic Information Policy." *Temple Law Review*, Vol. 63, No. 2, pp. 201 – 250.

Perritt, H.H. (1989a). "Electronic Acquisition and Release of Federal Agency Information: Analysis of Recommendations Adopted by the Administrative Conference of the United States." *Administrative Law Review*, Vol. 41, Summer, pp. 253 – 314.

Perritt, H.H. (1989b). "Government Information Goes On-Line." *Technology Review*, Vol. 92, No. 8, November/December, pp. 60 – 67.

Privacy Commissioner of Canada (1991). *Annual Report of the Privacy Commissioner, 1990 – 1991.* Office of the Privacy Commissioner of Canada, Ottawa, Ontario, Canada, June.

Privacy Commissioner of Canada (1990). *Annual Report of the Privacy Commissioner, 1989 – 1990.* Office of the Privacy Commissioner of Canada, Ottawa, Ontario, Canada, June.

Privacy Commissioner of Canada (1989). "Data Matching Review." A resource document for notification of the Privacy Commissioner of Proposed Data Matches. Office of the Privacy Commissioner of Canada, Ottawa, Ontario, Canada, July.

Prosser, W.L. (1960). "Privacy." California Law Review, Vol. 48, pp. 383 – 423.

Province of British Columbia (1991). *Land Information Management Framework.* Ministry of Environment, Lands and Parks, Surveys and Resource Mapping Branch, Victoria, B.C., Canada, October.

Province of New Brunswick (1990). "A Discussion Paper on the Right to Information Act." Fredericton, New Brunswick, Canada, November 1990.

Roitman, H. (1988). "Public Record Laws: A Proposed Model for Changes." *Proceedings of the 1988 Annual Conference of URISA. Mapping the Future,* Vol. IV, Ed. L.C. Williams. Los Angeles, California, U.S.A., 7 – 11 August, pp. 338 – 347.

Rymer, J.R. (1990). "Security Services: Standing Between Chaos and Order in Distributed Environments." *Patricia Seybold's Network Monitor*, Vol. 5, No. 12, December.

Salmon, E.E. (1989). "Constructing the Legal Risk Decision Matrix for GIS Recovery Models." *Proceedings of the 1989 Annual Conference of URISA. Charting the 90s: New Visions for Urban Technology,* Vol. IV, Ed. W.F. Gayk. Boston, Massachusetts, U.S.A., 6 – 10 August, pp. 293 – 304.

Saskatchewan Property Management Corporation (1989). Interim Policy on the Distribution of Digital Base Map Information. Central Survey and Mapping Agency, Regina, Saskatchewan, Canada, September.

Schweitzer, J.A. (1990). *Managing Information Security: Administrative, Electronic and Legal Measures to Protect Business Information.* Butterworths, Boston, U.S.A.

Science Council of Canada (1990). *Innovation and Intellectual Property Rights in Canada.* Ottawa, Ontario, Canada, March.

Shattuck, J. and M.M. Spence (1988). "The Dangers of Information Control." *Technology Review*, Vol. 91, No. 3, April, pp. 62 – 73.

Snapper, J.W. (1989). "Whether a Misuse of Computer Technology is a Violation of Personal Privacy." In *The Information Web: Ethical and Social Implications of Computer Networking*, Ed. C.C. Gould. Westview Press, Boulder, U.S.A., pp. 71 – 86.

Soloway, S. (1980). "Public Access to Commercial Information in Government Files." Commission on Freedom of Information and Individual Privacy Research Publication No. 17, Toronto, Ontario, Canada.

Sookman, B.B. (1989). "Liability of Owner, Creator and Distributors of Computer Data Banks and Networks." *Proceedings of the 1989 Annual Conference of URISA. Charting the 90s: New Visions for Urban Technology,* Vol. IV, Ed. W.F. Gayk. Boston, Massachusetts, U.S.A., 6 – 10 August, pp. 256 – 276.

Summers, R.C. (1989). "Local-Area Distributed Systems." *IBM Systems Journal,* Vol. 28, No. 2, pp. 227 – 240.

Toffler, A. (1980). *The Third Wave.* Pan, London.

Treasury Board of Canada (1990a). Management of Government Information Holdings Policy. Ottawa, Canada, August.

Treasury Board of Canada (1990b). Government Communications Policy. Ottawa, Canada, October.

Trottier, P. (1988). "Third Party Information: Too Many Protections? or Too Few?" Proceedings of *Key to the 90s: Privacy and Information Access.* Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, 22 – 23 November, pp. 15 – 16.

Vermont Office of Geographic Information Services (1991). "Public Access." Vermont Geographic Information System Policies, Standards, Guidelines, and Procedures Handbook, Part 1, Policies, Section B. Montpelier, Vermont, U.S.A., March.

Wacks, R. (1989). *Personal Information: Privacy and the Law.* Clarendon Press, Oxford.

Webster, C. (1988). "Disaggregated GIS Architecture: Lessons from Recent Developments in Multi-Site Database Management Systems." *International Journal of Geographical Information,* Vol. 2, No. 1, January/March, pp. 67 – 79.

Westin, A.F. (1967). *Privacy and Freedom.* Antheneum, New York.

Wilkinson, M.A. (1991). "Extending Freedom of Information and Privacy Legislation to Municipalities in Ontario." *CISM Journal,* Vol. 45, No. 3, Autumn, pp. 383 – 391.

Legislation Cited

Access to Information Act, R.S.C. (1985) c. A-1.

Copyright Act, R.S.C. (1985) c. C-42.

Criminal Law Amendment Act, Statutes of Canada (1985) c. 19.

Data Protection Act, Statutes of the United Kingdom (1984) c. 35.

Electronic Communications Privacy Act, 18 U.S.C. 2510 (1986).

Freedom of Information Act, Statutes of the Commonwealth of Australia (1982) c. 3.

Freedom of Information Act, 5 U.S.C. 552 (1974).

Freedom of Information and Protection of Privacy Act, Statutes of Ontario (1987) c. 25.

Freedom of Information and Protection of Privacy Act, Statutes of Saskatchewan (1991) c. F-22.01.

Municipal Freedom of Information and Protection of Privacy Act, Statutes of Ontario (1989) c. 63.

Official Information Act, Reprinted Statutes of New Zealand (1988) v. 21.

Open Records Act, Alaska Statutes (1990) c. 200.

Open Records Act, Iowa Code (1989) § 22.2.

Open Records Act, Kentucky Revised Statutes (1990) § 61.960 – § 61.975.

Patent Act, R.S.C. (1970) c. P-4.

Privacy Act, Statutes of the Commonwealth of Australia (1988) c. 119.

Privacy Act, R.S.C. (1985) c. P-21.

Privacy Act, 5 U.S.C. 552a (1974).

Right to Information Act, A.N.B. (1978) c. R-10.3.

Appendix I

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

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 unauthorized 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

i) within a reasonable time;

ii) at a charge , if any, that is not excessive;

iii) in a reasonable manner; and

iv) 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.

Appendix II

Australian Privacy Act (1988) Information Privacy Principles

14. 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 I 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 I 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.

Appendix III

ACUS Recommendation 88-10

A. Freedom of Information Act

1. In interpreting the Freedom of Information Act, agencies should recognize that a "record" includes information maintained in electronic form.

2. Agencies using electronic databases rather than paper records should not deny access to the electronic data on the grounds that the electronic data are not "records:' that retrieval of the electronic information is equivalent to creation of a "new" record, or that programming is required for retrieval. In responding to FOIA requests, agencies should provide electronic information in the form in which it is maintained or, if so requested, in such other form as can be generated directly and with reasonable effort from existing databases with existing software. Agencies, however, should not be obligated under the FOIA to create large new databases for private advantage, thus using agency resources for private purposes. Agencies should use a standard of reasonableness in determining the nature and extent of the programming that provides an appropriate search for and retrieval of records in responding to FOIA requests, and in determining the extent to which FOIA requesters may ask the agency to produce data organized in formats other than those used by the agency in the regular course of its operations.

3. Differences in technologies and database structures used by individual agencies make it necessary, for the near term, to define FOIA obligations on a case-by-case basis. Further experience with electronic information systems is a prerequisite to the formulation of general rules applicable to such controversies under the Act as how requesters must identify the records sought, how much programming, if any, an agency must do, and how costs shall be borne. The concept of reasonableness applied to searches for paper information made in response to FOIA requests should provide a useful guideline for resolving controversies over the application of FOIA to electronically maintained data.

B. Acquisition of Information in Electronic Form

1. Agencies should acquire information in electronic form when they use, or will use, the information in that form and when most information submitters already maintain information electronically, or have ready access to intermediaries who will prepare and submit it in electronic form. When agencies sponsor electronic acquisition programs, they should make clear their intention that all information required will eventually be available to them in electronic form, either by strictly administering exceptions to mandatory programs, or by undertaking the conversion of paper submissions into electronic form themselves.

2. When most providers of information ("filers") are technologically sophisticated, it is appropriate for agencies to require electronic filing of information, after developing standard formats in consultation with the filer community, and after appropriate testing and transition periods.

3. In determining whether to require or permit electronic filing of information and in designing the particulars of an electronic acquisition program, agencies should carefully weigh the costs and benefits of electronic acquisition of information. The analysis should address the factors identified in Recommendation D together with other considerations made relevant by the agency's mandate.

4. Agencies initiating electronic acquisition programs should take steps to facilitate electronic filing by entities having limited technological capacity (without raising the costs for sophisticated entities), including the optional use of "smart forms." When a significant proportion of the filer community is technologically unsophisticated, electronic acquisition may be feasible only through intermediaries. In such cases, agencies should create economic incentives for electronic filing rather than mandating it. Part of the economic incentive to file electronically under voluntary electronic acquisition programs can be the imposition of a fee on technologically sophisticated filers who choose to file on paper, assuming the statutory authority to do so exists.

C. Release of Information in Electronic Form

1. Electronic information release policies should depend on such factors as (a) whether the desired level of release consists of electronic publishing, electronic disclosure, or electronic access in response to FOIA requests (see the glossary for definitions of these terms); (b) the agency's policies in releasing like information maintained in paper records; and (c) the costs and benefits of replacing or supplementing an existing paper medium with an electronic medium.

2. When a statute or agency policy mandates the publishing of information, the agency should itself electronically publish the information or facilitate its electronic publication by others, unless the cost-benefit analysis suggests the desirability of restricting publishing to the paper medium, possibly accompanied by a lower level of electronic release.

If the agency publishes the information only on paper, it should consider electronic publication of the availability of the paper information products. Where an agency publishes information electronically, it should consider the feasibility of providing dial-up access.

3. When a statute mandates public reference room disclosure, or paper products presently are made available through a public reference room, agencies should provide electronic disclosure in public reference rooms of information already in electronic form. Such agencies should consider the costs and benefits of upgrading from electronic disclosure to electronic publishing. Agencies should also make information disclosed electronically available to any requester in an electronic form that would be easily usable by information resellers.

4. In those instances where an agency maintaining information in electronic form has no mandate to release information other than in response to FOIA requests, the agency should consider upgrading release of appropriate parts of this information to electronic disclosure through public reference rooms and wholesaling in electronic bulk form to private sector requesters

D. Allocation of Responsibilities Between Public and Private Sectors

1. Agencies that have decided under Recommendations B and C to acquire or release information in electronic form should define the appropriate roles of the public and private sectors in providing that information and related products (including telecommunications facilities, indexes and retrieval software as well as raw data). That choice should depend on the relative costs and benefits of privately versus publicly provided information products.

2. When choosing between publishing and a lower level of electronic release of information, an agency should determine whether private sector providers are willing to supply electronic products having features (e.g., user-friendly menus) that will give the public greater benefits or lower costs than would electronic publishing by the agency. When an agency relies on the private sector for electronic publishing of agency information, the agency should seek to establish by contract the nature of the products to be provided.

3. When an agency determines that its mission warrants new electronic means of acquisition or release of information and the private sector will not commit to provide them at appropriate prices, the agency should provide them, if clearly identified non-economic and economic benefits outweigh the capital and marginal costs. Agencies should recognize, however, that there may be circumstances where the costs to an agency would suggest the wisdom of creating incentives for the private provision of the desired electronic information product – for example, the free use of agency-developed software.

E. Determination of Costs and Benefits

1. Agencies should take into account the following costs in the decision making processes suggested in Recommendations B, C and D:

(a) Capital costs to the agency of establishing the product, and the probable economic life and other uses over which the costs should be allocated;

(b) Capital costs to information consumers and information providers to utilize the product, and the probable economic life and other uses over which these costs should be allocated;

(c) The marginal costs to the agency for user access;

(d) Marginal costs to users for obtaining the information;

(e) Marginal costs to electronic information providers of updating the electronic information;

(f) Unrecovered costs associated with existing government or private sector capital that would be made obsolete by the new product;

(g) The costs of updates and upgrades in service levels or capacity necessary to permit intended benefits to be realized at levels of demand expected over the long term; and

(h) Costs of changing to standard formats or of handling different formats.

2. Agencies should take into account the following benefits in decision making processes suggested in Recommendations B, C and D:

(a) Savings associated with eliminating the cost of producing and maintaining existing paper products;

(b) Savings to agencies and consumers associated with upgrading the level of information release from ad hoc FOIA disclosure to electronic disclosure in a public reference room;

(c) Savings to agencies and consumers associated with upgrading paper public reference room disclosure to electronic publishing;

(d) Increase in the number of interested persons having access to information;

(e) Improvements in the utility of information for its intended purpose because of improved organization and retrieval capabilities; and

(f) Reductions in delays associated with transferring information from an agency to eventual consumers.

3. Cost-benefit analyses should take into account FOIA obligations, including obligations to protect trade secrets and other exempt information. In designing electronic databases, agencies should consider the types of FOIA requests likely to be received for data in the database, consulting with representative users when feasible. Insofar as it is consistent with agency mission performance, databases should be designed so as to facilitate responses to FOIA requests. A proper rule of thumb is that it should not be any more difficult to obtain information under the FOIA after automation than before.

4. In some cases, effective design may require some sacrifices in electronic FOIA retrieval capability. In these cases, agency designers of electronic databases and retrieval software should consider how FOIA requests can be satisfied consistent with the spirit of the Act. For example, an agency might choose to make raw data available to requesters in computer-readable form along with retrieval software, so that requesters can effect their own retrievals. In other situations, new electronic information products may reduce costs of FOIA requests, to both requesters and agencies. This would occur, for example, if information were published or otherwise made accessible electronically in a public reference room, rather than provided only on paper in response to FOIA requests.

F. Exclusive Control of Public Information

An agency generally should not grant a private party exclusive control of its electronic information or of the acquisition or release thereof Nor should the agency itself as a general matter maintain such control in the absence of a compelling public purpose. Where an agency has, and wishes to exercise, authority to enter into an exclusive arrangement providing a private sector vendor with a preferential right to electronic information, the agency should first consider whether the analysis suggested in Recommendations B, C, D and E demonstrates that efficiencies can be achieved through such an arrangement The agency should also guard against the possibility that the arrangement may be inconsistent with its responsibilities under the FOIA or may impair the ability of the agency and the public to benefit from subsequent technological developments.

G. Technology Issues

1. Agencies should use proven technologies in their electronic acquisition and release systems. They should stay abreast of the state-of-the-art in all matters related to the electronic acquisition and release of information and should be particularly alert to the need for up-to-date and effective access control and other techniques required to maintain an appropriate level of security.

2. Agencies should seek to base electronic information formats on existing standards efforts such as American National Standards Institute standards on Electronic Business Data Interchange before developing their own distinctive format definitions.

3. Whenever possible, agencies should use public data networks rather than developing their own communications links for public filers or consumers.

4. Agencies should consider conducting demonstration projects to experiment with evolving electronic information technology.

H. Electronic Participation in Administrative Proceedings

Agencies should experiment with electronic means of providing public participation in rulemaking, adjudication and other administrative proceedings, while retaining a means of effective participation for persons who lack the means to access the electronic information system.

I. Government-wide Policy on Electronic Information

1. A government-wide policy on electronic information is desirable to afford guidance to agencies. Such a policy should articulate goals consistent with those expressed in the foregoing recommendations.

2. Congress should formulate the larger value judgments necessary for a government-wide policy on electronic information. These include the roles of public and private sectors; who ought to pay for increased information utility; and the level of funding to be provided by the government.

3. Because agencies often are in the best position to apply the considerations identified in this recommendation, Congress should normally defer to agency judgment in selecting methods to implement congressionally enacted policies when the agencies have offered rational justifications for their electronic information program decisions.

J. National Institute of Standards and Technology

The National Institute of Standards and Technology should continue to work with the U.S. Patent and Trademark Office to advance electronic data storage and transmission technology, as, for example, its work with high-capacity storage technology, and should inform agencies about commercially available products and services to facilitate electronic acquisition and communications.

Vita

Candidate's full name	:	Ralph Ian Anderson.
Place and date of birth	:	Berri, South Australia, November 6, 1965.
Permanent address	:	47 Corunna Avenue Colonel Light Gardens, 5041 South Australia.
Current employer	:	South Australian Dept. of Lands G.P.O. Box 1047 Adelaide, 5001 South Australia.
Schools attended	:	Unley High School Adelaide, 1978 – 1982.
Universities attended	:	South Australian Institute of Technology The Levels, 1984 – 1987 Bachelor of Applied Science (Surveying).
		University of New Brunswick Fredericton, N.B., Canada, 1990 – 1992 Master of Science in Engineering.